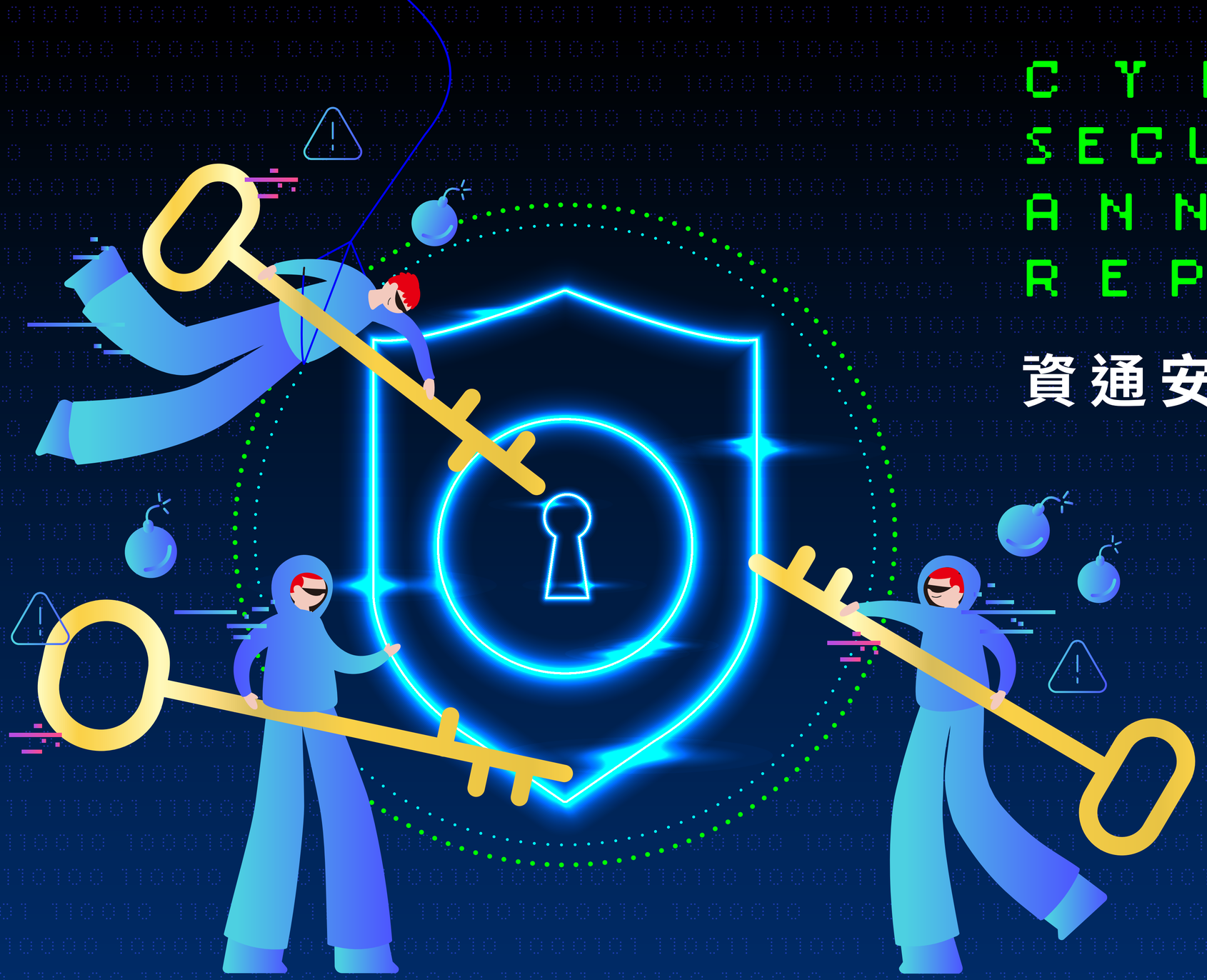
twcertcc

CYBER SECURITY ANNUAL REPORT

資通安全年報



2022

TABLE OF CONTENTS

CYBER SECURITY ANNUAL REPORT

CHAPTER 1

前言

1 前言

近些年來對全球資安而言是個充滿動盪及破壞的時期，各國政府及企業持續於資安疫情大流行的未知水域中航行，要到達安全“新常態”還有很長的路要走；如同預測一樣，惡名昭彰的 SolarWinds 漏洞風險仍然在，在這份 2022 年報中，我們揭示了關鍵攻擊媒介與技術，諸如：反射放大流量的 DDoS 攻擊、借道第三方的供應鏈攻擊、Log4Shell 漏洞等，這些都能讓駭客以小博大造成目標對象的巨大損失。此外，科技應用變革也伴隨著新的挑戰，數位轉型的浪潮急遽推上高峰，遠距工作打破網路邊界、WEB 3.0 去中心化應用程式、分散式資料儲存、物聯網裝置普及、社群媒體與行動支付結合，都面臨著嚴峻的安全與隱私問題。

TWCERT/CC 持續對國內企業組織分享資安情資，依類型區分前兩名為漏洞訊息、威脅清單，第三名則為系統疑存在弱點，代表我國仍有大量系統存在被入侵的風險，企業組織加強資安意識刻不容緩。在各類資安風險中，未經授權存取及外部入侵屬重大類型，與此相關之勒索軟體攻擊逐漸成為主要手法，如今，並成為勒索軟體即服務 (Ransomware as a Service, RaaS) 的模式，具有動態入侵途徑、檔案加密鎖定及資訊揭露雙重勒索等特性。隨著 RaaS 的出現，勒索攻擊不僅只是靠釣魚郵件或少數幾種漏洞進行入侵，企業組織的每一個資訊設備與人員皆可能成為被利用的目標。針對於此，TWCERT/CC 建立勒索軟體專區，提供事前防護、事中處理、事後回復各階段措施指南，以提升資安防護能力。另方面，我國是資通訊軟硬產品重鎮，2022 年期間共計接獲 101 個資安漏洞，產品範圍涵蓋軟體服務系統、IoT 設備與伺服器等，我們協調各相關廠商，助其對產品進行軟韌體之修補更新。

駭客攻擊企業的威脅從不停歇，新的資安破口需要及早防堵，資安不能是個防疫孤島，這是個全球攜手合作的聯防議題，TWCERT/CC 扮演著國內、國際間資安情資分享暨事件通報角色，2022 年間總計分享逾 110 萬筆之資安情資予相關單位。此外 TWCERT/CC 也持續與國內外資安組織及企業定期並即時地進行情資交流分享，提升我國資安聯防能量。TWCERT/CC 亦透過惡意檔案檢測平台 – Virus Check，協助大眾檢測檔案中是否藏有惡意程式，降低遭社交工程惡意檔案攻擊之機率。此外，並辦理 2022 年通報應變年會活動，採實體與線上方式同步進行，以「資安韌性，營運永續」為主題，國內外與會嘉賓達九百餘人；此外，針對國內中小企業需求，於全台七縣市辦理了「資訊安全防護及案例分享研討會」活動，對提升企業界資安認知及政策制定意義重大。

CHAPTER 2

資安威脅與防護

2.1 企業組織之資安威脅與防護

2.1.1 TCP Middlebox 反射放大 DDoS 攻擊趨勢與防護

反射放大 DDoS 攻擊簡介

分散式阻斷服務 (Distributed Denial-of-Service, DDoS) 攻擊，為駭客發送大量的網路封包或服務請求，使得受害系統或主機因頻寬無法負荷或資源耗盡而癱瘓，導致不能提供正常服務。

DDoS 攻擊主要可分為頻寬消耗及資源消耗兩種攻擊類型，一般新聞媒體所報導之巨大流量攻擊多屬於頻寬消耗類型，此類型攻擊者會透過傳送大量無效的服務請求給受害主機或伺服器，使得網路頻寬壅塞，導致一般使用者無法順利登入或連線，產生主機或伺服器癱瘓之後果。

攻擊者通常會利用大量的殭屍電腦同時發出攻擊，而要產生如此大流量的攻擊，仍是一個難度很高的挑戰，於是出現了反射放大的攻擊技術，透過中介設備或服務將初始流量放大後送給受害者，其放大倍數從數倍到上百倍不等，也因此近年來屢屢刷新攻擊流量紀錄，本文所探討的 Middlebox 反射放大攻擊即為此類的新型攻擊技術。

Middlebox 反射放大 DDoS 攻擊簡介

近期因 Middlebox 設備漏洞研究而興起的 DDoS 攻擊技術，國內企業採用了相當多的相關設備，故於本節介紹該攻擊技術概念。

網路通訊的設計原則之一，是由通訊雙方的終端設備來解析並處理封包，傳輸過程中所經過的網路設備僅負責將封包送往正確的目的地，不查看或修改封包內容。

然而因應 Internet 的快速發展，為了解決網路擴展的瓶頸、提升傳輸效能、增加通訊安全等目標，網通業者在網路設備上引進流量操控的功能，用於檢查、過濾、更改封包，已不僅是轉發的功能，這種類型的網路設備稱為 Middlebox。常見的 Middlebox 設備有網路位址轉譯器 (Network Address Translation，NAT) 、內容過濾系統 (Content Filtering System)、入侵偵測／防護系統 (Intrusion Detection/Prevention System，IDS/IPS)、代理及反向代理 (Proxy/Reverse Proxy) 等。

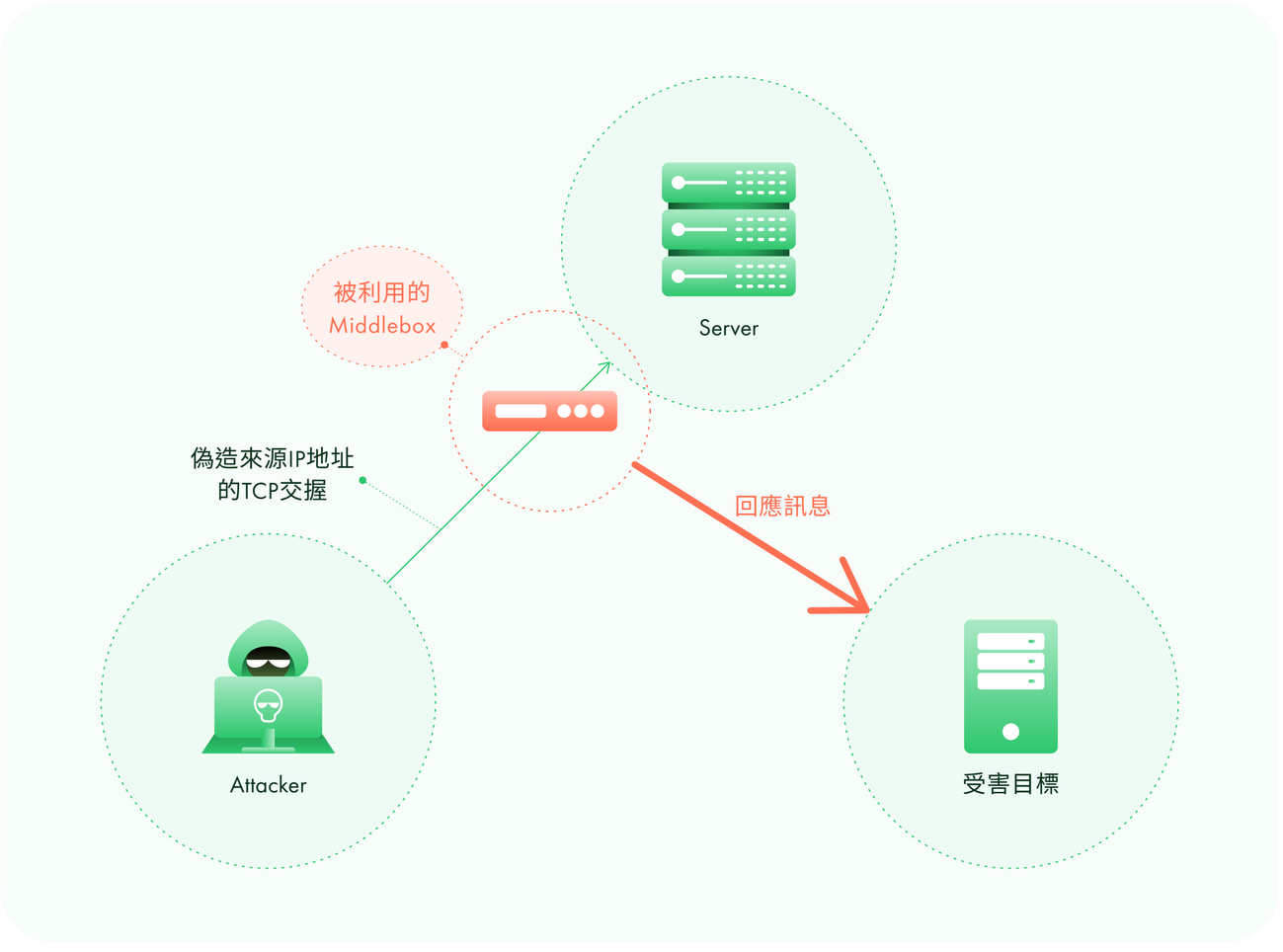
Middlebox 反射攻擊的機制

Middlebox 反射攻擊的設計思維來自於設備不會確認 TCP 三向交握的正確性，因此 Middlebox 反射攻擊是一種 TCP 的反射式攻擊，利用 TCP 的 Middlebox 反射攻擊基於下列三項要素：

1. 攻擊者將服務請求夾帶於 TCP 三向交握封包內（特別是 TCP SYN）
2. Middlebox 無視 TCP 三向交握封包不應夾帶服務請求，仍然正常的進行後續處理流程
3. 後續處理流程中，Middlebox 在回應請求時，處理了被夾帶的服務請求內容，導致回應內容大增，形成放大攻擊

傳統的反射放大攻擊之所以無法藉由 TCP 來進行，是因為攻擊者送出的服務請求必須仰賴正常的 TCP 連線，而在偽造來源 IP 位址的前提下，TCP 連線是絕對無法被成功建立的，但在 Middlebox 的利用上，是在 TCP 三向交握內夾帶服務請求，放入了可被放大的資料。

圖 1：利用 Middlebox 的 TCP 反射放大攻擊

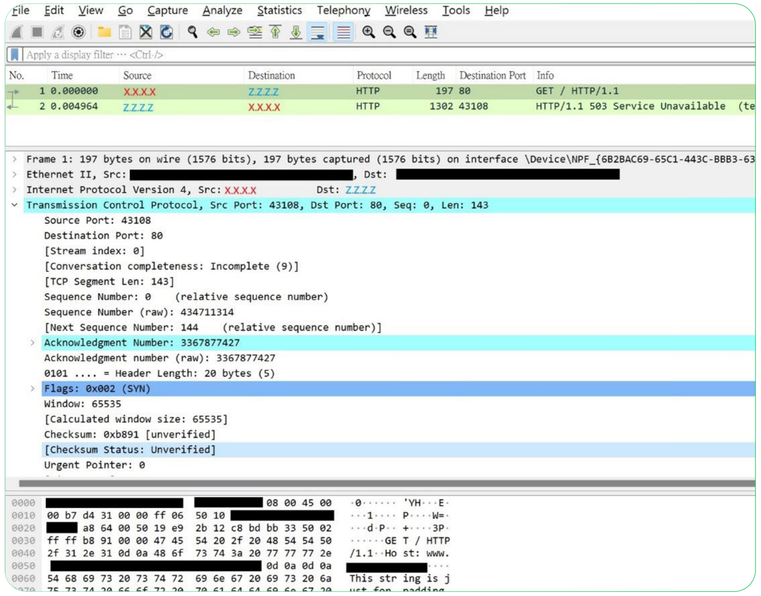


資料來源：TWCERT/CC 整理

國內案例與防護建議

圖 2 及圖 3 是一個位於台灣的 Middlebox 被用作 TCP 反射放大攻擊的例子。圖 2 顯示攻擊者發出一個 TCP SYN 封包，其中來源 IP 位址偽造成受害目標的 IP 位址 X.X.X.X，目的 IP 位址 Z.Z.Z.Z 為某 Middlebox 保護的伺服器所分配到的對外 IP 位址。這個 TCP SYN 封包夾帶了載荷，內容是一個 HTTP GET 請求，存取不存在的 URL。

圖 2：攻擊者發送一個帶有 HTTP GET 請求的 TCP SYN 封包

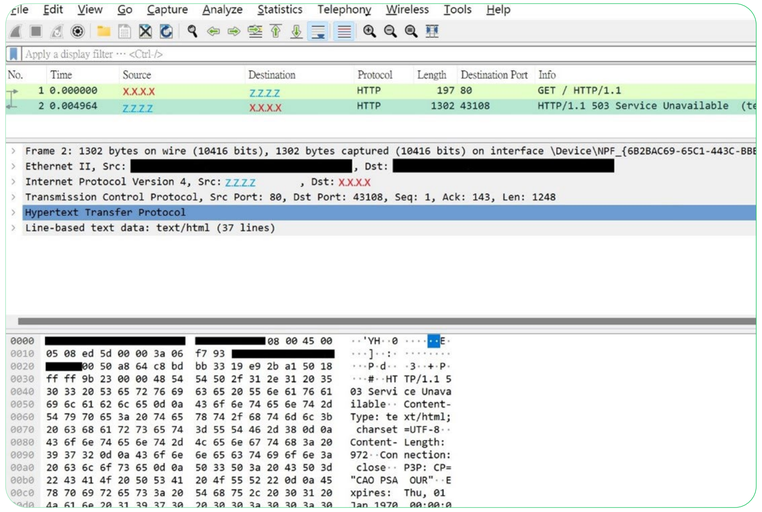


資料來源：TWCERT/CC 整理

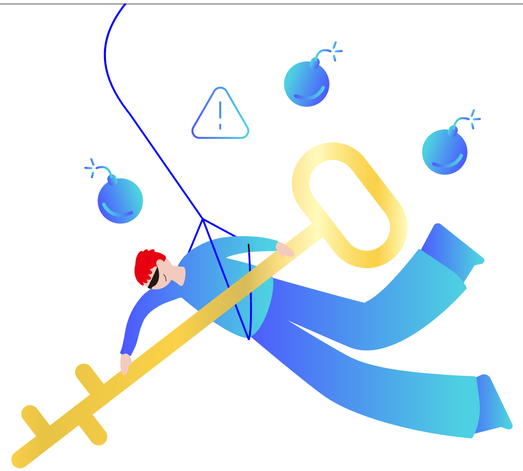
Middlebox 收到這個 TCP SYN 封包之後，回應了一個 HTTP 狀態碼 503（服務無法使用）的封包，其中夾帶一個網頁附帶許多錯誤資訊；整個封包大小為 1302 bytes。

此時並沒有正常的 TCP 連線被建立，但 Middlebox 仍然回了一個 PSH, ACK 封包給受害目標。

圖 3：Middlebox 將回應反射給受害目標



資料來源：TWCERT/CC 整理



在這個案例中，攻擊者送出 143 bytes 的資料，而 Middlebox 回應了 1248 bytes 的資料給受害目標；單就 payload 而言，放大了 8.7 倍。事實上，攻擊的放大倍率仍可再提高，如在攻擊者送出的 TCP SYN 封包夾帶較多數量的資料；例如將夾帶的資料量改為 100 bytes，那麼此例的放大倍率即超過 12 倍。

Middlebox 在網路架構中的角色定位即是分析防護機制，因此很難有完美的 Middlebox TCP 反射放大攻擊的防護方法，因為這涉及 Middlebox 設計通則－許多 Middlebox 就是被設計作為只檢視特定方向的封包流，而忽略流經的封包是否屬於正常的 TCP 連線。然而仍可從以下緩解手段減輕或是避免某些 Middlebox 被利用的可能。

從 Middlebox 本身調整緩解

採用可檢視雙向流量的 Middlebox

部分作為內容過濾的 Middlebox 其功能整合在網路 Gateway 裡。這種 Middlebox 有能力判斷 TCP 連線狀態，而只處理或是將資訊注入到那些已建立有效 TCP 連線的封包裡。

1

將要注入到封包內的警告或說明資訊，降到最低的大小

部分 Middlebox 在攔截到敏感資訊的存取要求時，以完整網頁的形式注入了大量資料到回覆封包裡，造成很高的放大倍率。建議調整這種情況下的回覆資料量，或是將回覆的網頁實作在另一台網頁伺服器上，而 Middlebox 僅送出一個 HTTP redirect 封包。

2

只過濾向外的流量

部分 Middlebox 的目的不在於保護內部網路資源，而在於限制內部網路設備對外部網路資源的存取。例如，某些管理政策嚴格的企業，禁止員工在公司內部網路瀏覽 Internet 上的特定資訊。這種情況下，Middlebox 就無須對由外部網路流往內部網路的流量進行攔截並作出回應，以避免被外部攻擊者利用作為反射攻擊。

3

不作任何的放大

只讓 Middlebox 回送一個 RST 來關閉連線也是一個簡潔有力的方式。

4

從防火牆進行緩解

上面幾點是針對 Middlebox 的緩解措施。如果 IT 或網管人員無法對 Middlebox 進行設定，就只能嘗試由防火牆的 ACL 來阻擋可疑封包：丟棄任何流入的、帶有載荷的 TCP SYN 封包。Akamai 提供了一個作為參考的防火牆 ACL [1]：

deny tcp any eq 80 host x.x.x.x match-all +syn -ack packet-length gt 100

注意事項如下：

攻擊者可能對任一埠發送帶有載荷的 TCP SYN 封包。上述防火牆 ACL 作為參考用途，只顯示作用於埠 80 的情況，可參考調整。

1

攻擊者發送的 TCP 封包，不限定於 SYN。上述防火牆 ACL 作為參考用途，只顯示作用於 TCP SYN 封包的情況，可參考調整。

2

攻擊者發送的偽造封包不一定會大於 100 bytes。正常不帶載荷的 TCP 封包，大小多為 60 bytes。上述防火牆 ACL 作為參考用途，只顯示了作用於封包大於 100 bytes 的情況，可參考調整。

3

2.1.2 供應鏈資安與零信任之威脅與防護

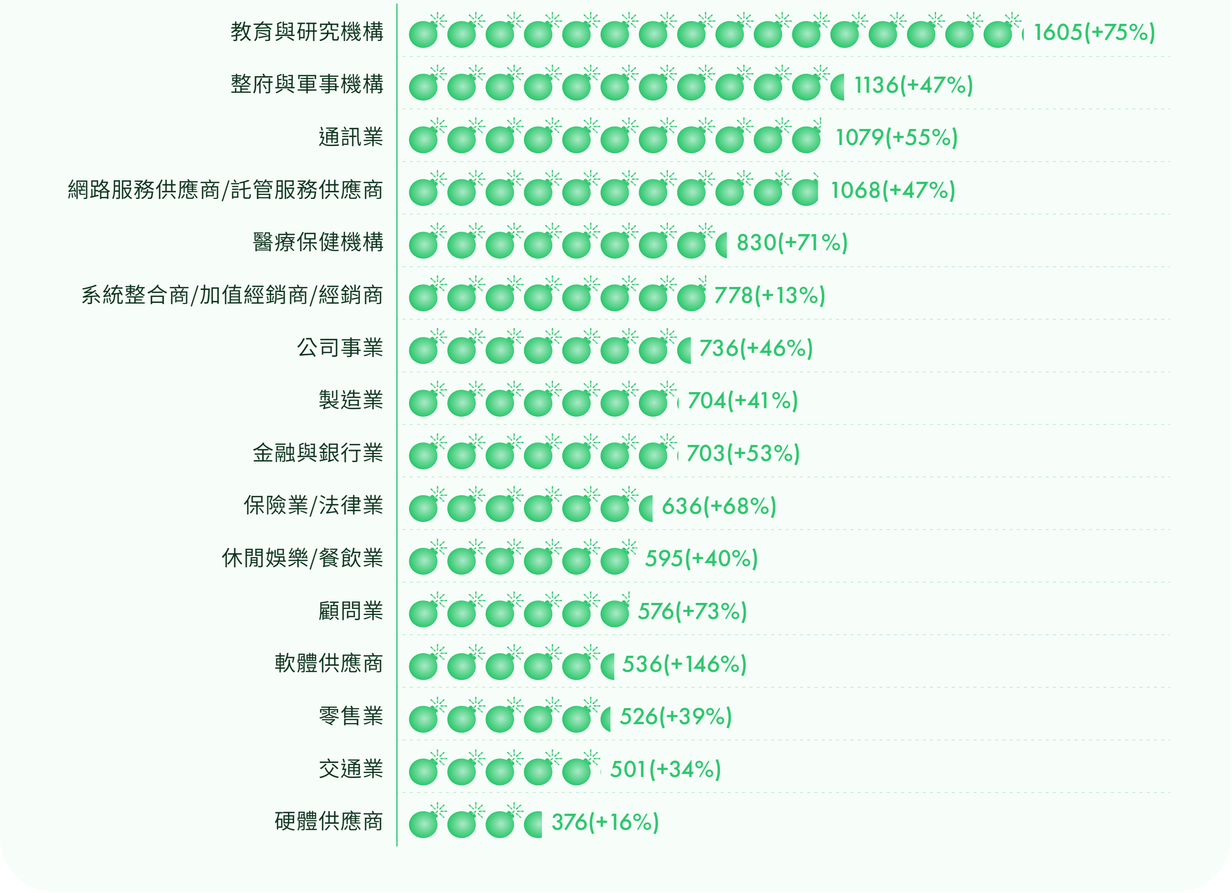
供應鏈資安簡介

供應鏈攻擊 (Supply Chain Attack) 是一種間接入侵目標的攻擊方式，網路犯罪分子會透過找尋與攻擊目標所合作的第三方服務供應商，並利用可以橫向至單位的途徑進行攻擊。近些年供應鏈攻擊頻傳，自 2020 年的 SolarWinds 攻擊、2021 年的 Codecov、Kaseya 攻擊與 Log4j 漏洞事件中皆可發現單一漏洞即可造成大範圍影響，也顯示供應鏈中固有的重大資安風險。

根據 Check Point Software 發布之 2022 年網路安全報告 [1] 指出，企業於 2021 年每週遭受網路攻擊的數量較 2020 年增長 50%。教育與研究機構首當其衝，每週遭受 1,605 次攻擊，年增 75%；其次為政府和軍事機構，每週遭受 1,136 次攻擊（增長 47%），以及通訊業的 1,079 次攻擊（增長 51%）。其中軟體供應商所遭受的攻擊次數增幅最大，與 2020 年同期相比增長了 146%，這與 2021 年軟體供應鏈攻擊趨勢不斷增長有密切關係。相關攻擊趨勢如右圖所示。

趨勢科技於 2022 年資安年度預測報告 [2] 中指出，駭客可能發展出 “四重勒索” 的攻擊模式，除了傳統勒索攻擊中透過將企業檔案加密、外洩敏感資料及發動 DDoS 攻擊影響企業營運等恐嚇手段之外，未來恐利用供應鏈信任圈發動攻擊，透過軟體、韌體、硬體植入惡意程式，鎖定企業配合的供應商及委外廠商進行大規模攻擊，更甚至販賣透過攻擊供應鏈所取得存取憑證的存取服務 (Access-as-a-Service)。也因此，供應鏈資安已成為 2022 年持續應正視的焦點。

圖 4：2021 年企業遭受攻擊趨勢



資料來源：CheckPoint

供應鏈威脅面向

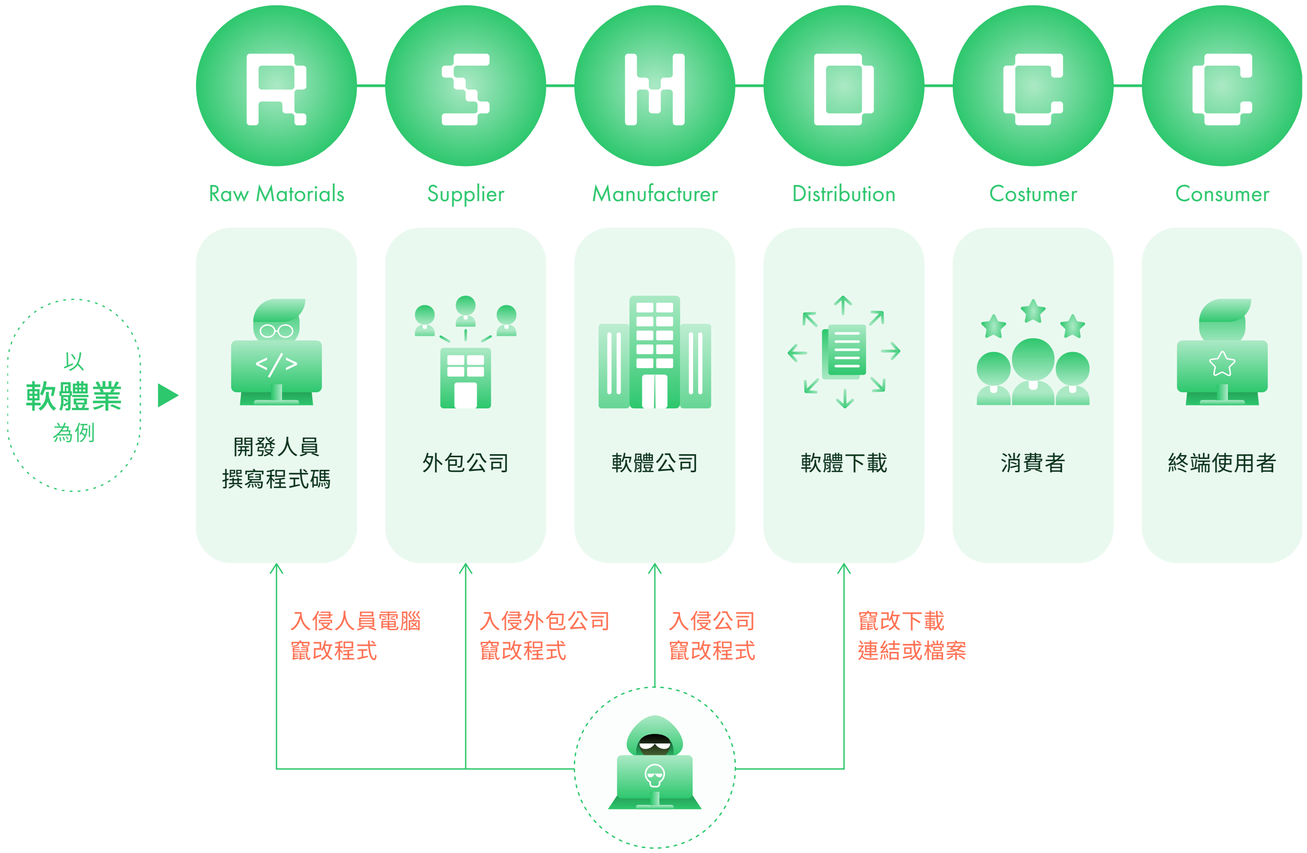
供應鏈威脅泛指企業的產品或服務，在開發生命週期的任何階段，讓攻擊方得以實現存取、間諜活動和營運活動之破壞。駭客通常從供應鏈中安全防護較弱的環節進行攻擊。根據國內外供應鏈攻擊案例以及其攻擊途徑，常見的供應鏈攻擊可歸納為以下兩個威脅面向：

1. 駭客透過入侵特定軟韌體開發公司或委外人員之電腦，進行竄改程式或是下載連結等行為，造成大範圍感染與擴散。

2. 駭客入侵開發廠商後，以開發廠商設備做為跳板，再利用開發商與目標單位之間的信任管道，如 VPN、遠端桌面等，進行入侵與散播惡意程式。

以軟體業為例，所可能面對的供應鏈威脅如下圖所示。駭客可透過入侵供應鏈資安較脆弱的環節進行攻擊。 例如開發人員電腦、外包公司、軟體公司皆有可能遭受駭客入侵竄改程式，或是竄改軟體下載連結或檔案，造成消費者及終端使用者遭受惡意程式攻擊。

圖 5：供應鏈威脅面向



資料來源 : NCCST[3] | 資料來源 : TWCERT/CC 整理

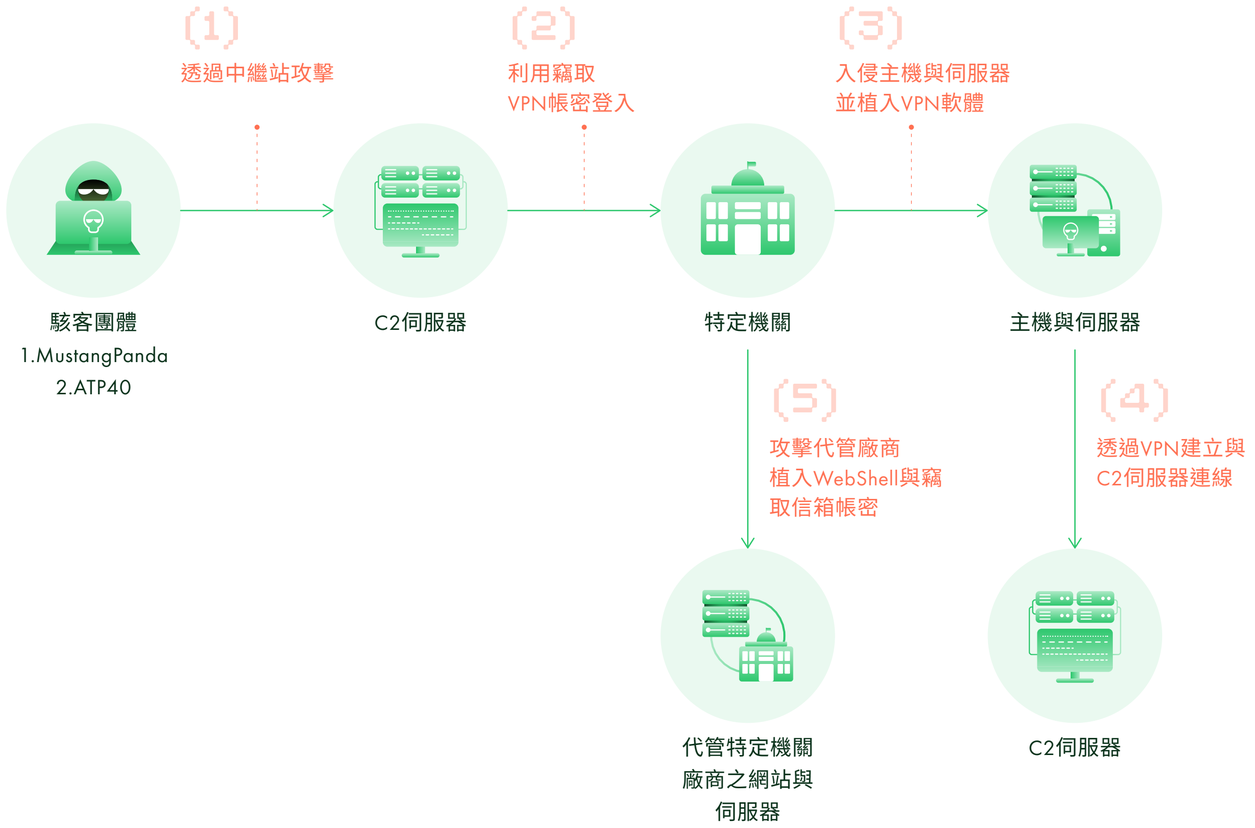
以下章節將針對國內供應鏈攻擊事件進行探討：駭客透過入侵人員電腦及外包公司進行攻擊的台灣資訊供應鏈攻擊事件。

台灣資訊供應鏈攻擊事件

此案例為駭客透過竊取外包廠商 VPN 登入帳密入侵的供應鏈事件。自 2018 年起台灣陸續發生特定機關被駭客入侵攻擊事件，根據調查結果顯示，駭客組織 Blacktech、Taidoor、MustangPand 和 APT40 利用特定機關提供遠端桌面存取權限、VPN 登入等機制作為跳板，入侵特定機關網路，試圖竊取機敏資訊。由於國內委外案為求便利，經常提供委外廠商遠端桌面連線、VPN 登入等機制，方便委外資訊服務廠商進行遠端操作與維運。此外，國內廠商未部屬資安防護設備，或無資安人員之配置，也易形成資安破口。

在此次事件中，駭客組織 Mustang Panda 與 APT40 攻擊流程如下圖所示。駭客組織首先透過 C2 伺服器 (1)；竊取的外包廠商 VPN 帳密，進行遠端登入特定機關網路 (2)；取得其管理權限帳號，再進行橫向擴散入侵特定機關內部主機及伺服器，植入 VPN 軟體 (SoftEtherVPN)(3)；並回報 C2 伺服器與回傳資訊 (4)；接著入侵資訊廠商代管特定機關之網站與郵件伺服器，取得信箱帳號等機敏資訊 (5)。

圖 6：駭客組織 MustangPanda 與 APT40 攻擊流程



資料來源：TWCERT/CC 整理

而駭客組織 Blacktech 與 Taidoor 於此事件中鎖定與台灣特定機關合作之委外廠商，攻擊流程如下圖所示。首先以其所使用之含有漏洞的網路路由器設備作為入侵點，取得該路由器控制權作為惡意程式中繼站 (1)；再透過破解員工 VPN 帳號密碼與釣魚郵件攻擊等途徑，入侵資訊服務廠商 (2)；並將竊取的資訊回傳至駭客中繼站 (3)；接著透過安裝 VPN 程式再向其他客戶 / 特定機關進行攻擊與擴散 (4)；被入侵的客戶 AD 伺服器以群組原則派送惡意程式 Waterbear 至其他設備 (5)；最後受害之設備向中繼站連線並回傳資訊 (6)。

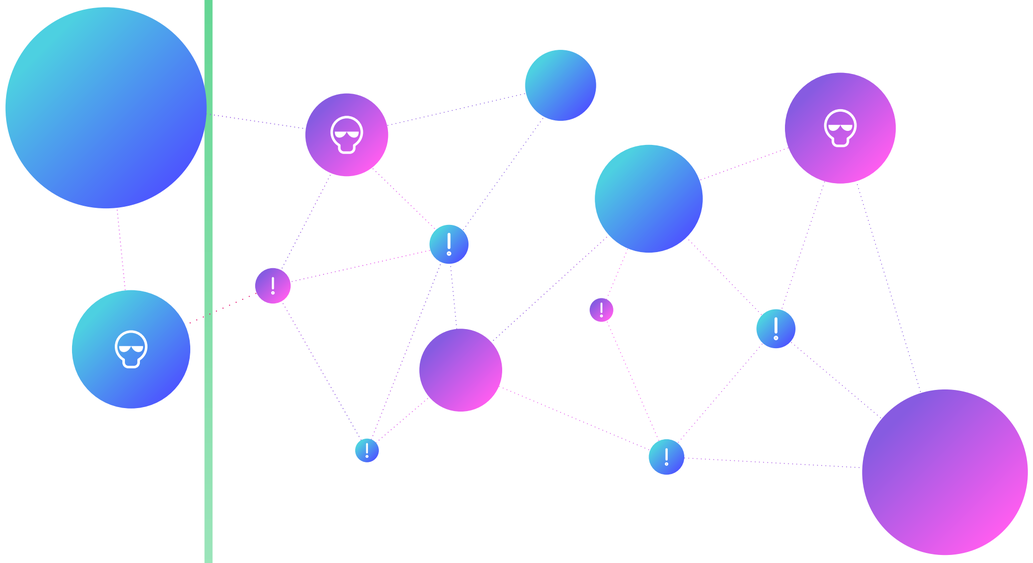
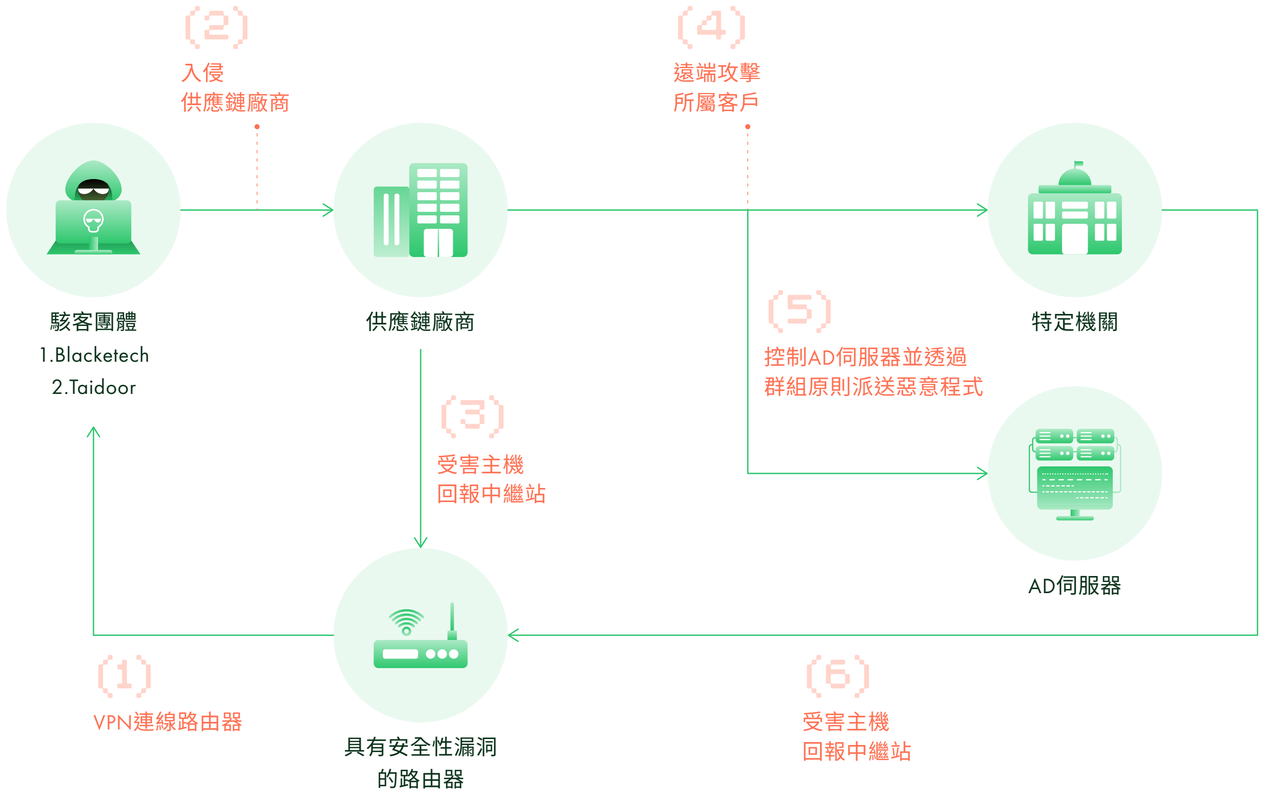


圖 7：駭客組織 Blacktech 與 Taidoor 攻擊流程



資料來源：TWCERT/CC 整理

我國供應鏈資安規範與因應措施

台灣為 ICT 及 IoT 等智慧產品製造重鎮，為確保供應廠商產品與使用者端之安全，數位發展部施行以下措施，以強化我國供應鏈防護能力：

1

制定「關鍵電信基礎設施資通設備資通安全檢測技術規範」

2

開發通傳事業資通設備資安漏洞通報系統

在 (1)「關鍵電信基礎設施資通設備資通安全檢測技術規範」中，現數位發展部指定防火牆、交換器、路由器須做實機測試與資料備查。在實機共同測試的項目中，強調系統弱點及漏洞檢測。

在 (2) 通傳事業資通設備資安漏洞通報系統中，電信商需要定期盤點有哪些資通設備，清單需上傳至 C-ISAC，並由 C-ISAC 自動通知電信業者 CVE 待修補資訊。

國內企業等組織導入零信任之建議方式

供應鏈攻擊可能發生在科技產品開發生命週期的任何階段，所以在產品生產的規劃之初，就必須從產品開發生命週期的需求分析、設計、開發、測試到維護階段中，納入資通安全防護考量與措施。國內目前有國家資通安全研究院，提出零信任網路架構之概念驗證，但因相關元件伺服器與 API 尚無完整功能的開源解決方案，有賴相關系統廠商開發推出，相關資訊可參考國家資通安全研究院官網的零信任專區。若需於現階段導入零信任網路架構的企業組織，建議可參考 NIST SP 800-207 所建議之零信任導入方式，而實務作法則可參考美國 NCCoE(National Cybersecurity Center of Excellence) 所介紹的幾種應用網路架構以及相關協作廠商。

在 NIST SP 800-207 指出，零信任架構的導入是漸進過程，並非全面翻新，大多數的導入狀況將會混合零信任架構與傳統邊界防護方式，在混合架構的狀況下，將會逐步依個別業務推動導入。因此，為了避免重複建置，業務間共通常用的功能應該要先進行檢視，例如身分驗證、日誌記錄、裝置管理等功能，如能較為彈性的設定或微調，可更有效率的同時支持傳統架構與零信任架構。若是無法共同使用或是需要重新設計，則可盡量參考 SP800-160v1 的系統安全建議來進行。而導入過程將包括對資產、業務流程與流量狀況進行識別、分配盤點等動作，才能進行後續導入工作，而在調查盤點後，也需要定期維護。下圖為 NIST 建議的導入步驟。

圖 8：NIST 建議的導入零信任架構步驟

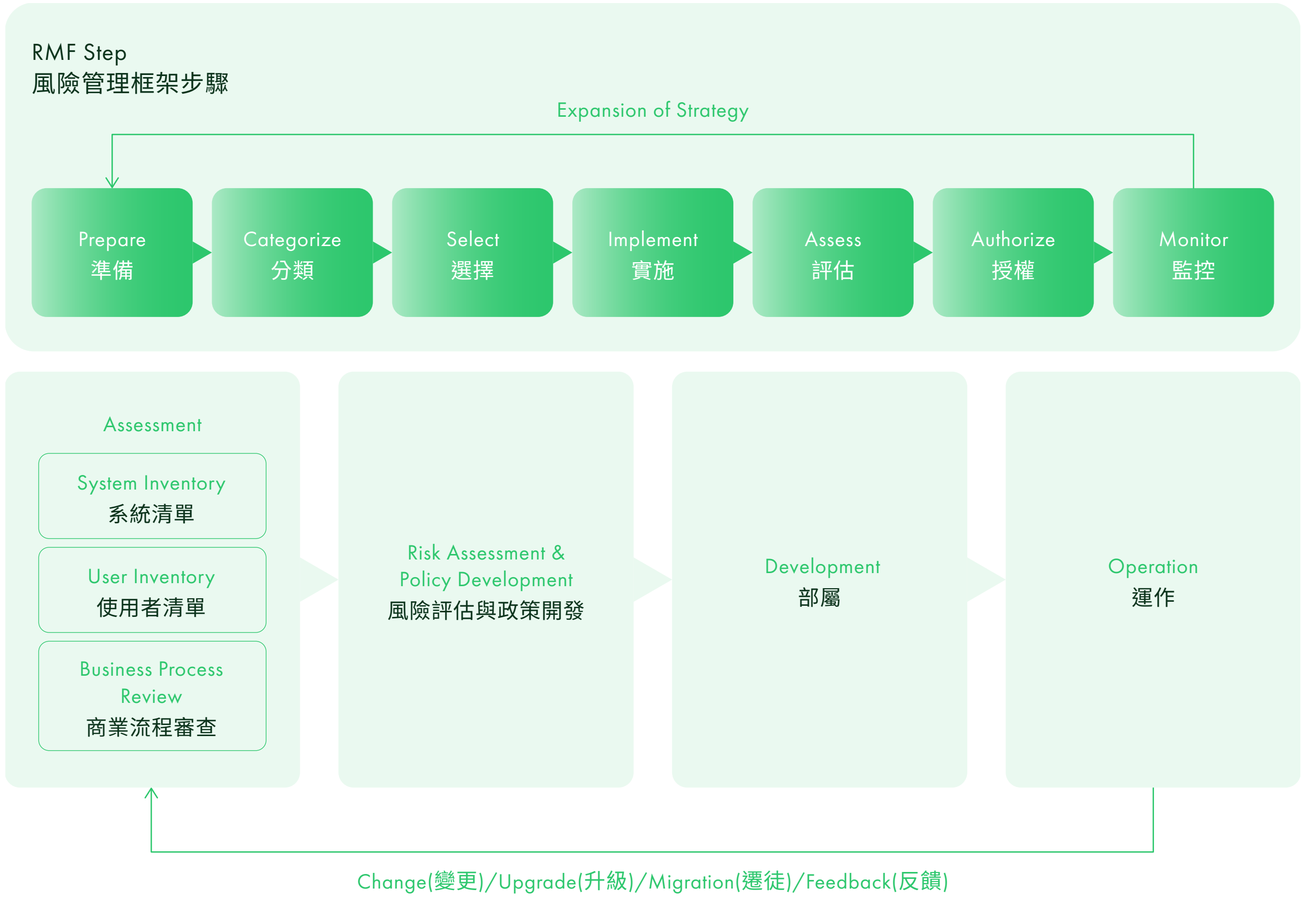


Figure 12 : ZTA Deployment Cycle

資料來源 : NIST"Zero Trust Architecture"

NIST 建議了導入零信任機制的 7 大步驟：1. 識別企業角色，2. 識別企業資產，3. 識別關鍵流程並評估執行風險，4. 為零信任角色制定政策，5. 識別解決方案，6. 初始化部署與監控方案，7. 擴展零信任架構。

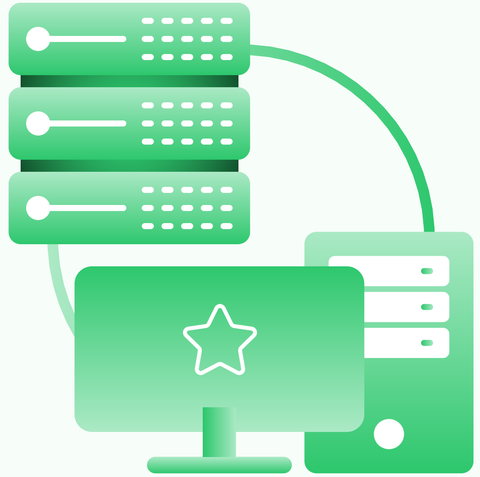
1

識別企業角色

把企業中的主體先識別出來是有其必要性，而主體不只是人，範圍更包括了資源、服務，甚至是帳號，而且在識別出角色，還需識別出該角色的特性、權限、重要性，才能規劃零信任架構下適當的存取方式。

而在導入的過程中，可以參考 NIST SP 800-63A 不同嚴格程度的標準做規劃，因應企業對資安的需求程度，或是服務的重要性，可以有彈性的作法。

2



識別企業資產

在識別出企業內的角色後，非企業所擁有的資產也需要識別與管理，在企業的網路設備中就可能存在非企業所擁有的部分，也就是意味著這些部分都能存取到企業內的網路。包括硬體，例如筆記型電腦、手機與 IoT 裝置；還有數位物件，例如使用者帳號、應用軟體與憑證等。這些未必是企業本身所有，可能租借或是因為服務需要而應用外界的資產。要完整的做到所有面向的盤點是瑣碎且不容易的，但還是要盡可能的盤點，且形成一套可用的管理與監控機制。

識別關鍵流程並評估執行風險

在識別完企業內外的角色、資產後，接著要擴大到流程面，也就是企業的業務流程、資訊處理流程、業務間關係，要進行識別並找出關鍵的節點。

因為零信任架構針對傳統企業內部也進行信任關係的切分，導致業務流程中間的環節被各種存取或驗證機制所切斷，這在傳統上是不會發生的，在零信任架構下，每個存取都可能需要通過不同等級的驗證要求，通過不同的資安政策評估，導致可能被拒絕的結果。

所以導入零信任架構時， 必須要瞭解到各種流程的關鍵節點所在，並對中斷時的處理方式進行考量與規劃，以維持業務的營運，在導入初期，建議從較低重要性的業務流程開始，累積熟悉零信任所帶來的影響，再逐步推展。

而導入零信任所需要考慮的不僅是業務的中斷，更應該要將效能、使用者體驗，以及增加流程風險一併加入規劃，並評估取捨，才能順暢的運行零信任架構。

為零信任角色制定政策

對企業中的角色也如前一點所說明的，要對角色所在的業務流程、重要性、關聯角色、使用資源有所瞭解，再制定與角色相關的政策或處理動作，這裡也牽涉到風險的評估，可參考 NIST SP 800-37 風險框架。

識別解決方案

確認資產、角色與流程後，接下來進行整體規劃的解決方案，這部分 NIST 提供 5 個關鍵角度可以參考。

是否要求在非企業資產中加入資安元件？

在非企業資產使用時可能會造成限制，例如對行動設備提出 BYOD 相關要求，就會造成更多額外的資安支出與流程。

是否須考量業務流程的存放運行場所？

資源有可能是在雲端，也可能是在近端，這會造成業務流程的差異，在資安面向上也會因此有所差異，影響到零信任在政策與工具 (如驗證方法) 使用的選擇。

是否有可供分析的 Log ？

零信任架構會不斷持續的檢討與調整決策，因此需要流程中各種 log 來做為參考。

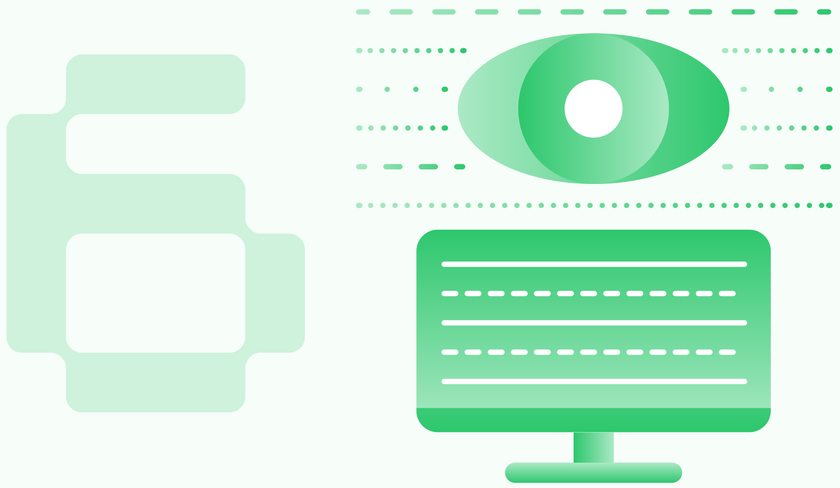
是否能廣泛的支援應用軟體、服務與協議？

意即零信任所採用的解決方案支援程度不同，會產生不同的實作方法，例如網路、SSH 支援廣泛，而 IPv4 也是大多情況下共通的協定，但不是每個方法都如此通用。

是否會改變主體的行為？

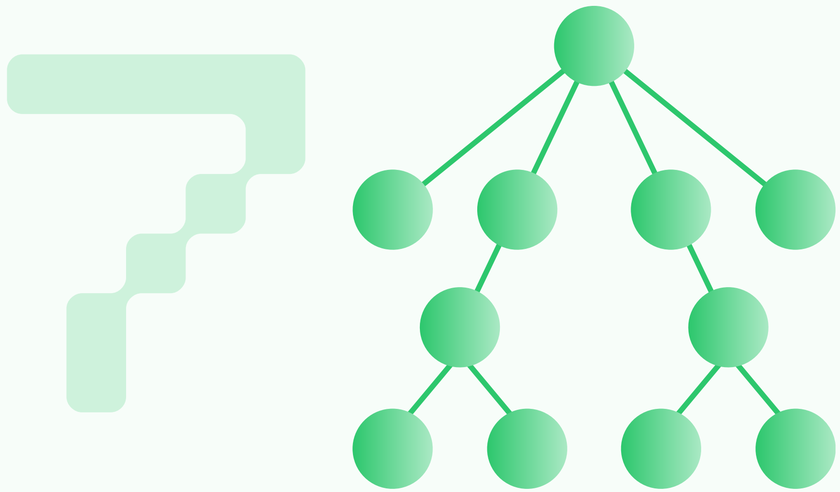
因為對流程有所變動，或在節點中加入各種驗證需求，導致額外的步驟，會改變到整個企業主體既有的執行方式。

這些考量面向是建議先挑選部分業務做為測試，從各個小部分累積導入經驗，再總合規劃整個企業的導入，逐步脫離傳統架構。



初始化部署與監控方案

導入初期通常無法一次到位，可先採用監控與通知的方式來進行，業務流程依據零信任架構所規劃的作法來進行，但在發生存取拒絕或是政策衝突時，就只產生報告來做記錄，不會真的拒絕存取動作，這樣一段時間後，就可以確認解決方案有效或是找出問題，同時也讓企業內的角色慢慢理解其運作原理，同時也能檢視記錄的有效性，再滾動檢討政策規劃。



擴展零信任架構

過了初期測試監控的階段後，已對流程的影響有所習慣，並且使政策趨於完善，此時會逐步真正的實施控制的動作，而不僅止於監視與通知，此時，也會再次檢討真正實施後對企業帶來的影響，再進行修正調整，同時也會擴大實施零信任架構的範圍，直到成功導入為止。

2.2 網路應用之資安威脅與防護

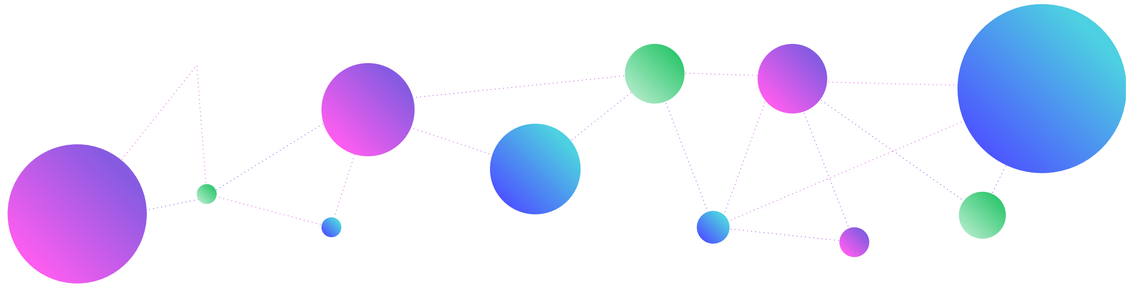
2.2.1 WEB 3.0 技術與資安風險

WEB 3.0 簡介

網際網路經過數十年的發展，已成為人們日常生活中必不可少的一部分。而最初做為共享資訊，及交換訊息目的所建立的全球資訊網(World Wide Web，WWW，或簡稱為 Web)，迄今已深刻地改變了社會的溝通模式，協助人們實現了跨地域的政治、產業及文化的各種交流，並促進了各領域科技技術的創新與擴散。

自上世紀 90 年代的第一階段全球資訊網 Web1.0 時代開始，HTML(HyperText Markup Language，超文本標記語言)、URI(Uniform Resource Identifier，統一資源標識符) 和 HTTP(HyperText Transfer Protocol，超文本傳輸協定)，構成了全球資訊網的基本技術，並促進了靜態網站開始蓬勃發展。此一時期的靜態網站，主要是由企業組織創建和控制，數據資料和網站內容是由靜態文件系統 (而不是資料庫) 提供的。隨著社交媒體平台、論壇及部落格的出現，Web2.0 時期開始於 2004 年，並成為當今網站技術的主流。Web2.0 最大的演變，是讓網站不再是如同 Web 1.0 一般，只是單向提供資料，而是演變為可讀寫的。網路公司開始提供平台來共享使用者產生的內容，並參與使用者之間的互動。這些資訊共享的平台，卻牢牢控制在網路公司手中，從使用者閱讀的內容、購買的產品、觀看的娛樂節目到人與人之間的交流方式，都受到大型科技公司控制。加上層出不窮的個人資料外洩及濫用案例，引發了人們對網路去中心化的呼籲。

於是，全球資訊網的第三次迭代，Web3.0(或稱為 Web3)，由以太坊聯合創始人 Gavin Wood 於 2014 年提出，其背後的理念是消除 Web2.0 網路巨頭的中心化主導地位，以便將資料數據的控制權交還使用者，創造一個去中心化的網路世界。



WEB3.0 技術介紹

Web3.0 特色

由於 Web3.0 是一個基於區塊鏈技術的去中心化開放網路，雖然區塊鏈 (如以太坊) 的節點可以為智慧型合約提供處理能力，但用以託管使用者資料數據、NFT 圖像及其 Z 他可以支援 dApp 的文件，卻需要一套分散式資料儲存系統，以便讓使用者能夠控制自己的資料數據及其分布，解決資源中心化所引起的一系列問題 (如安全及隱私受到潛在侵犯、資料集中而導致的單點失效問題等)。

1

去中心化

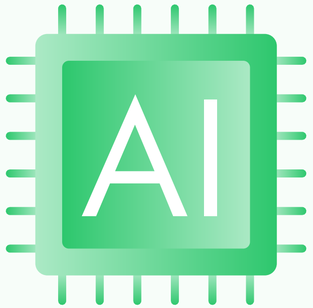
去中心化是 Web3.0 的核心目標，它試圖改變 Web2.0 時代中，資料數據或服務儲存在固定網路位置 (如 IP) 上的形式，以致使用者首先需要知道伺服器的網址 (URL)，才能透過 HTTP 等協定獲取相關服務。在 Web3.0 中，資料數據或服務託管在分散式資料儲存系統中，而不是在網路公司所控制的伺服器上，因此可以同時在多個網路位置建立副本，使用者可以根據內容找到相關的資料副本。

2

無需信任和無需許可

去中心化應用程式 dApp (Decentralized Application)，允許在智慧型合約 (smart contract) 的基礎上，構建使用者所需的服務，為使用者提供無需信任 (trustless) 和無需許可 (permissionless) 的體驗。由於基於智慧型合約的 dApp 可以在區塊鏈 (如以太坊) 上自行運行，dApp 意味著使用者不需要信任任何一個網站平台，即可依靠智慧型合約來正常工作。

3



人工智慧 (AI) 和機器學習

在 Web3.0 中，通過基於語意網 (Semantic Web) 的概念 (如在文件添加能夠被電腦所理解的語意)，及自然語言處理的技術，電腦將能夠像人類一樣理解信息。Web3.0 將利用資料和演算法來模仿人類的學習方式，逐步提高其準確性。這些功能將使電腦能夠在藥物開發，及新材料等許多領域產生更快、更相關的結果。

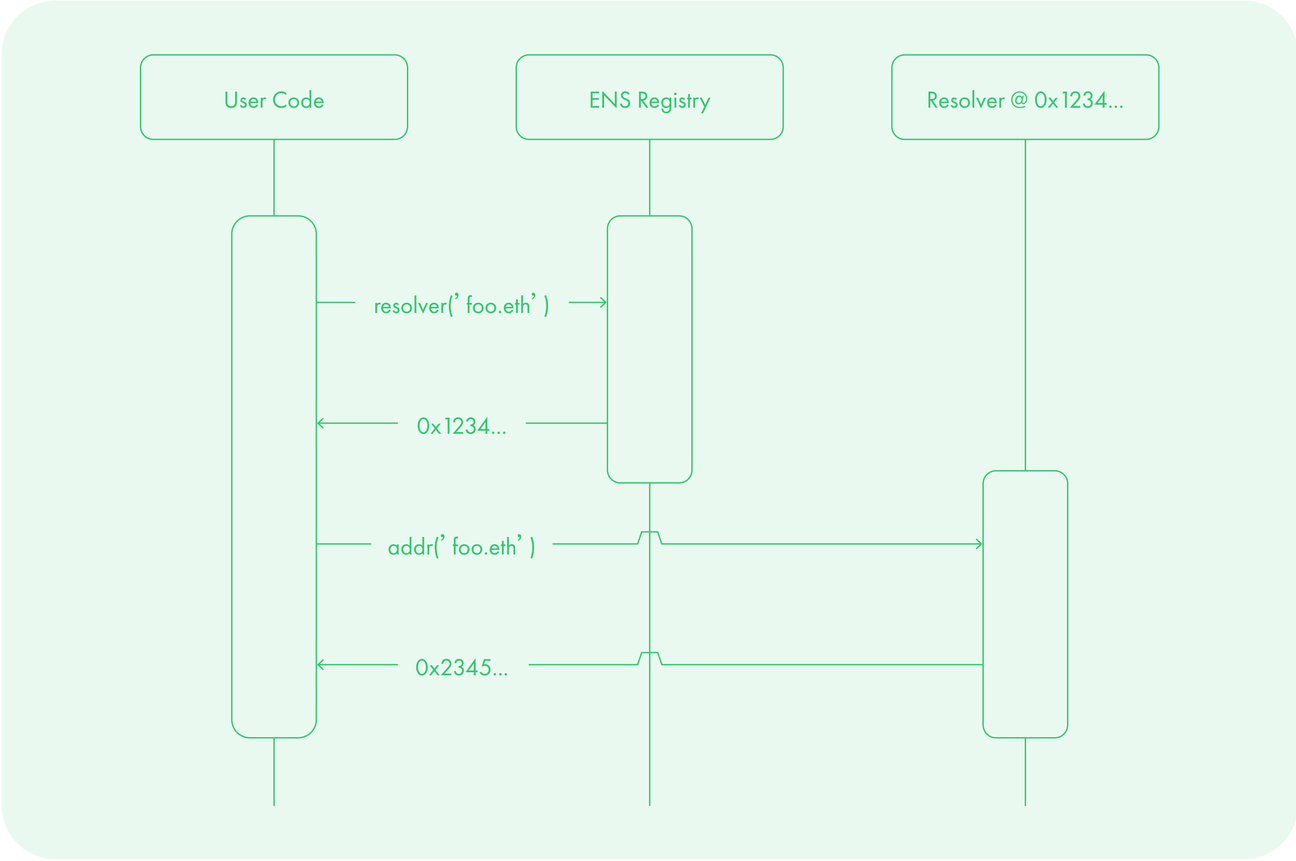
ENS 技術研析

IPFS 針對文件內容所計算的雜湊值，會成為該內容的永久地址，放入區塊鏈交易中。但因為該內容地址難以被普通使用者記憶 (例如：0x4fc2dC4f1F253416Fde25a9Aa8676ec11364cfdc)，故可使用去中心化域名服務 ENS (Ethereum Name Service)，將該地址映射 (mapping) 至 ENS 域名 (例如：myDocument.eth)，讓任何人都更容易使用 ENS 域名進行內容存取，而無需輸入完整的十六進制地址。ENS 是一個開放的、分散式及可擴展的名稱系統 (naming system)，存在於以太坊區塊鏈的智慧型合約上，用以直接與以太坊區塊鏈互動。

ENS 為網站、dApp 及更多的 DWeb(Decentralized Web，去中心化網路) 打開了方便存取的大門，讓這些資源 / 服務可以通過去中心化、抗審查 (censorship-resistant) 和使用者控制的域名系統進行存取。ENS 的核心由 ENS 註冊表 (registry)，及解析器 (resolver) 兩個主要部分組成。首先，ENS 註冊表存在於運行在以太坊區塊鏈上的智慧型合約中，並記錄了所有域名 (domain) 和子域名 (subdomain)。ENS 的第二個關鍵是解析器，負責將 ENS 域名轉換為底層使用的 ETH 地址或文件內容雜湊值。這些也是區塊鏈上 ENS 智慧型合約的任務，例如當使用者欲存取 myDocument.eth 時，ENS 則回應 0x4fc2dC4f1F253416Fde25a9Aa8676ec11364cfdc。

ENS 的架構和運作流程可以概述為：當使用者欲解析 ENS 域名時，首先需在 ENS 註冊表中查詢 ENS 域名，然後註冊表回覆應該查詢哪個解析器，並且負責將域名轉換為地址的解析器，將最終的內容地址回覆給使用者 (如右圖所示)。

圖 9：ENS 域名解析過程



資料來源 : ENS Documentation

IPFS 技術研析

由於 Web3.0 的分散式資料儲存系統 ~IPFS(Interplanetary File System，星際文件系統) 協定，提供了 Web3.0 的使用者，實現資料儲存去中心化的目標。

IPFS 具有以下的技術特色：

1

IPFS 的核心是一個分散式系統，用於儲存和存取各種文件、網站、應用程式及資料數據。IPFS 與網路傳輸層 (Transport Layer) 使用的議定無關，使得它可以通過各種傳輸層進行通信，包括 TCP、UDT、QUIC、TOR、藍芽等。

2

IPFS 的工作原理是取得一個文件，並以加密方式對其進行雜湊 (hash) 處理，因此使用者最終會得到一個非常小，且可重現相關雜湊值 (hash value) 的文件表示值，因此使用者最終的互動標的物是特定的資料，而不是伺服器；

尋找資料時 (如文件、照片等)，IPFS 與傳統的 HTTP 協定不同，IPFS 是通過該資料的雜湊值 (hash value) 來存取相關內容。當使用者想透過瀏覽器存取特定資料時，IPFS 會詢問整個網路，是否有節點擁有與此雜湊值對應的資料。此時在 IPFS 上擁有相應雜湊值的節點將回傳資料，以便讓使用者可以從任何地方存取這些資料。

3

當 IPFS 與區塊鏈協同運作時，使用者可以在 IPFS 上儲存大量資料，並將不可變的永久 IPFS 地址放入區塊鏈交易中。在此架構下，IPFS 將提供一個可公開存取的分散式資料庫，而區塊鏈使其可以公開驗證。

4

IPFS 具備防範 DDoS 的優勢，駭客（或網軍）DDoS 的目標不可能是分散式儲存節點，這太耗費成本。

在 Web3.0 中的 IPFS 則是更新且更徹底的去中心化方法，如果一個系統中，轉帳都是通過區塊鏈全部節點的客戶端來進行，其內容資料都是由 IPFS Desktop 或 Planet 傳輸，也就具備了 DDoS 無法攻擊的特性，因此在 Web3.0 的運用上，對 DDoS 有較佳的防禦架構設計。

資安議題探討

資安效益

Web3.0 作為一個去中心化的開源協定，在區塊鏈及 IPFS 的支援下，展示了無需中介即可實現安全的點對點互動 (point-to-point interaction)，並透過完全去中心化，讓使用者產生的資料，不會再被網路巨頭所壟斷。

Web3.0 潛在的資安效益說明如下：

1 提高安全性

由於沒有資料儲存中心，Web3.0 更有可能抵禦駭客攻擊和其他安全威脅。例如當網站遭受駭客的分散式阻斷攻擊 (DDoS) 時，藉由 IPFS 技術，使用者仍可以從其它節點中取得相同的網頁內容，故沒有單點失效所引發的網頁可用性 (availability) 問題。

2 提升隱私

隱私保護是 Web3.0 構建時的重要考量，透過區塊鏈的匿名功能，使用者的身分及所產生的資料關連性得以受到保護，從而提升安全及隱私性。

3 更大控制權

由於使用者 (即節點) 之間直接互動，以獲取彼此想要的資料，因此使用者比通過中介擁有更大的資料控制權。

4 使內容審查變得更加困難

儲存在 IPFS 上的文件，可能散存在很多地方，加上沒有中央機構可以限制任何使用者，使用或部署 dApp，從本質上最大限度地減少了政府機構，或企業組織審查文件內容的可能性，促進了言論自由、行動自由和財務獨立性。

潛在資安風險

隨著 Web3.0 技術內涵日益成熟，潛在的資安風險也被提出，新的技術帶來新的資安議題，而傳統的攻擊威脅也被轉化到新的技術中，因此在以下的 5 個面向上可能有潛在的資安風險。

ENS 資安議題

ENS 使查找加密貨幣錢包地址更為便利，這也會導致受歡迎與常用的域名被第三方註冊並轉售。因此，惡意的 ENS 使用者將會欺騙毫無戒心的受害使用者，讓這些使用者相信正在與合法組織進行互動。此外，這些 ENS 指向錢包地址，也讓任何人可以隨時檢查與該名稱相關聯的錢包的內容，帶來潛在的風險。

社交工程

影響 Web 3.0 使用者的絕大多數安全事件是關於加密貨幣錢包的社交工程攻擊。使用者可能被欺騙而分享了他們所擁有的“種子短語”，由於加密貨幣錢包如果丟失或損壞，使用者可以使用 12 到 24 個單詞的“種子短語”（本質上是他們的私鑰），來恢復錢包及其所有內容。所以任何知道種子短語（私鑰）的人都可以克隆 (clone) 加密貨幣錢包，並占為己有。因此，試圖竊取加密貨幣或 NFT 的犯罪分子就以此為目標。

鯨魚 (貨幣大戶)

鯨魚是持有大量加密貨幣或 NFT 的知名加密貨幣賬戶的別稱，據統計，40,000 個鯨魚所擁有的 NFT 佔總市場價值的 80%。詐騙者知道許多較小的投資者會關注這些鯨魚的錢包，因此對這些小投資者進行社交工程，讓他們投資於虛假項目上，進而詐騙資金。

智能合約

部分攻擊者是利用合法智能合約中的漏洞進行惡意行為，但也有不同的作法，那就是將自己編寫的惡意軟體以惡意智能合約代碼的形式放置在區塊鏈上，這個惡意智能合約具有所有標準智能合約功能，但實際則暗藏惡意行為。

潛在垃圾郵件增加

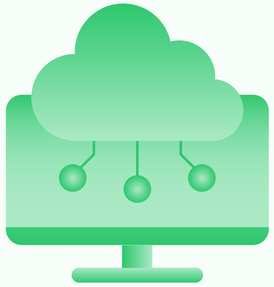
在 Web 3.0 中，搜索引擎、網站和 Web 應用程序將使用大量的網路資源作為資料庫，從這些資料庫中，使用者將得到想要的資料，但由於涉及大量資源，因此人們更容易染資源並通過該資源發送有害資料，使用者可能會收到損害系統的惡意腳本和勒索軟體，或是虛假訊息。

2.2.2 雲端資安威脅與防護

雲端資安簡介

隨著資通訊技術 (Information and Communications Technology，ICT) 不斷發展，日常的單一作業系統 (Operating System) 環境，已不足以有效利用電腦硬體日漸強大的運算能力，以致大部分時間機器多處在閒置狀態形成資源浪費。於是透過虛擬化技術，將單一硬體資源模擬成為多個虛擬機器 (Virtual Machine，VM)，使得每一個 VM 可以根據其應用所需，合理使用所分配到的運算資源，提高了硬體的利用率和靈活性。這種最初應用在大型主機 (mainframe) 上的虛擬化技術，在 2000 年左右開始快速發展，並伴隨著網際網路頻寬的提升、軟硬體革新，成為雲端運算的基礎。

在探討雲端資安威脅與防護議題前，首先需要瞭解雲端相關定義，本文採用美國國家標準暨技術研究院 (National Institute of Standards and Technology，NIST) 為雲端運算定義的五項基本特徵、四種部署模式和三種服務形式，簡述如下：



雲端運算的特徵

雲端運算的基礎架構，包括由硬體資源組成的物理層，和由跨物理層部署軟體組成的抽象層，其五項特徵為：

按需求的自助服務

使用者可以自行透過網頁介面，或行動應用程式取得服務，過程中無須通過資訊部門，或其他中間人協助。

快速彈性化的架構

彈性是指雲服務允許使用者在必要時，可以自行透過指定所需的主機配備及資源，如中央處理器、記憶體、頻寬、硬碟容量、作業系統等，動態創建使用者所需的服務，或為既有的服務增加或減少其所需的運算資源。

廣泛的網路存取方式

使用者應能夠從任何地方，透過支援可上網的設備存取雲服務，意味著筆電、平板、智慧型手機等攜帶型裝置，也可以便捷地存取雲服務。

可測量的服務

即雲服務提供了資源可以計量的功能，以便使用者可以合理地對所請求的資源付費，提高對雲端運算成本的控制。

虛擬化的資源池

將可能位於不同地點的實體 (如中央處理器、記憶體、硬碟、網路等) 與虛擬 (如作業系統、應用程式等) 運算資源，統一整合到一個虛擬化的資源池 (resource pool)，並透過多租戶模式 (multi-tenancy model)，將不同使用者所需的運算能力，從資源池中進行調配，讓使用者租用。

對許多規模大小不一的企業而言，企業可依據網路頻寬、計算能力或儲存空間的需要及預算，無縫地擴展或縮減運算資源。加上當今便捷的網路存取方式，讓企業可以遠端快速部署所需的運算環境，從而實現有效協作，提高生產力。

雲部署模型

有四種雲環境部署模型，使用者可以選擇最適合其需求的模型：

公共雲

在這種多租戶部署的模型中，公有雲為雲服務供應商 (如 AWS、Microsoft Azure 及 Google Cloud 等) 所有。眾多使用者共享公有雲的運算資源，並按資源使用量，付費給雲服務供應商。

私有雲

私有雲是為單個企業需求而建置的單租戶環境，安全性是其最顯著的優勢之一。私有雲所需的 IT 基礎設施，除了可以由企業自建在本身的資料中心內，也可以將其託管給專業的雲服務供應商。

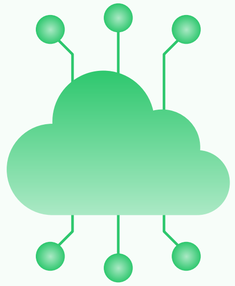
混合雲

由兩個或多個不同的公有或私有雲，透過標準化或專有技術，將彼此鏈結在一起，使資料和應用程式具有可移植性，以實現彼此之間的負載平衡。企業可使用此模型來補充其計算能力，例如，當私有雲的資料儲存容量，或計算能力不足，或臨時需要較大的頻寬時，企業可以利用公有雲來擴充私有雲的能力。相較於其他部署模型，混合雲提供了更大的靈活性、可移植性及可擴展性。衛福部的雲端資料中心，即為一成功案例，該中心透過混合雲將具有高度私密性的醫療資料，與各地區的醫療院所、衛生局、衛政單位等共享。

社群雲

由一群具有共同利益 (例如共同任務、策略和合規性需求，或有特定安全要求) 的企業，或特定使用者共同組成。相關的應用包括國內自行車製造龍頭，巨大集團工業導入的 Oracle 社群雲，用以即時掌握車友社群聲量與使用回饋，強化行銷成果。

無論是哪一種雲部署模型，企業使用雲端運算服務，其最主要誘因就是希望降低資本支出，並且可以在任何地方，透過網路高效率地營運。



雲端運算三種服務模式

基礎架構即服務 (Infrastructure as a Service, IaaS)

雲服務供應商負責管理虛擬化運算資源所需的基礎 IT 設施，並通過網際網路，將服務交付給客戶。雲服務供應商則負責讓企業可以存取和管理其需要的網路、伺服器、儲存空間，並提供所需的虛擬化技術服務。

平台即服務 (Platform as a Service, PaaS)

雲服務供應商在自己的 IT 基礎設施上，負責管理 (例如：更新及維護) 軟體及硬體，並透過網際網路將軟硬體以平台模式提供給消費者租用。PaaS 允許企業在租用的平台上，開發、運行和管理自己的應用程式，而無需建構和維護相關的平台或 IT 基礎設施。

軟體即服務 (Software as a Service, SaaS)

也稱為雲應用程式服務，雲服務供應商通過網頁瀏覽器，將整個應用程式租給消費者使用。雲服務供應商負責所有底層 IT 基礎設施的管理，包括軟硬體更新、資料儲存、備份、漏洞修補等。

上述三種雲端服務模式，對企業而言是一種 IT 營運觀念的轉移。雲端運算允許企業從雲服務供應商租用運算資源，而不是創建和管理自己的 IT 基礎設施，並且不需要支付伺服器採購、電力和機房使用與租賃等費用。由於雲服務供應商承擔了日常管理，和維護的繁重工作，因此為企業節省了大量時間、精力和金錢。

雲端資安案例與風險分析

從 NIST 所定義的雲端運算五項基本特徵、四種部署模式和三種服務形式來看，雲端運算帶給企業最主要的優勢，可以歸納成以下四點：

1. 運算資源的彈性取得。
2. 運算環境的快速部署。
3. 省卻軟硬體建置成本，及日常管理和維運的負擔。
4. 將 IT 基礎設施託管給雲服務供應商，企業可以將心力及資源專注在本身擅長的核心業務。

雲端資安案例

然而，企業在享受上述優勢的同時，也因雲端架構而帶來了資安風險，案例如下：

1

對資料、應用程式和服務的控制能力有限，以致完全擁有雲服務控制權的供應商，掌握了企業珍貴的資料。舉例來說，當企業採用公有雲，或託管給雲服務供應商 (如 MSP 業者) 的私有雲時，雖然雙方可以透過簽署終端使用者授權合約 (End-User License Agreements，EULA)，來保障彼此權益及資料的隱私，但是這種將資料文件，儲存在完全由第三方擁有和營運的伺服務器上，常常會為企業帶來潛在的資安風險。

相關著名的資安事件案例包括：

- 2017 年 4 月，PwC 與資安業者 BAE Systems 合作，揭發了一種名為「雲端跳躍行動」(Operation Cloud Hopper) 的駭客活動，指出惡名昭彰的駭客集團 APT10，藉由入侵 MSP 業者 (Managed IT Service Providers，IT 代管服務供應商)，取得系統管理員或網域管理員權限後，利用客戶之間共享 IT 基礎設施的特性，橫向移動竊取企業託管給 MSP 業者的機密資訊。由於 MSP 業者負責管理眾多客戶的 IT 基礎設施及服務，因此一旦 MSP 業者遭到入侵，則其旗下的客戶都將成為潛在受害者。
- 2018 年，一名前思科 (Cisco) 的工程師，入侵了思科託管在亞馬遜網路服務上的雲基礎設施，並故意刪除了數百台客戶託管的 WebEx Teams 應用程序的 VM，結果導致近 16,000 個 WebEx Teams 帳戶中斷長達兩週。事後，思科花費了 140 萬美元補救該事件所造成的損失，其中包括向受影響客戶退還的 100 萬美元。

2

國家通訊暨網際安全中心高度依賴雲服務供應商，以致一旦供應商出現問題時，例如發生網路連線中斷、身分驗證服務無預警失效、軟體更新錯誤、發生資安漏洞等，企業將可能馬上面臨營運停擺的風險。

相關著名的資安事件案例包括：

- 從 2018 年迄今，Google 共發生了 5 次嚴重的服務中斷問題，影響的服務包括 YouTube、Gmail、Google drive、Google maps 等服務，且這些服務中斷似乎都是全球性的。
- 國家通訊暨網際安全中心 2021 年 8 月，網路安全公司 Wiz 的研究人員發現微軟的 Azure Cosmos 資料庫 (ChaosDB) 資安漏洞，駭客能夠在其 ChaosDB 中，任意存取 Azure 上的任何 CosmosDB 帳戶，甚至刪除主要資料庫。微軟在收到通知後的 48 小時內消除了漏洞，並獎賞了 4 萬美元給發現漏洞並及時向微軟報告的研究人員 。
- 於 2021 年 12 月發生的 Log4Shell 漏洞 (CVE-2021-44228)，因駭客可以透過該漏洞，遠端執行任意程式碼，使得許多雲服務受到威脅。AWS 於去年發布的 Log4Shell 漏洞修補程式，被發現修補程式本身含有嚴重的資安問題，導致 standalone AWS 伺服器、Kubernetes clusters、Elastic Container Service (ECS) 和 Fargate 容易受到攻擊，AWS 經過反覆驗證後，最近才完成漏洞修補。
- AWS 在 2022 年 7 月發生電源故障，導致位於 US-EAST-2 區域的 AZ1 (Availability Zone 1) 內的服務中斷。該故障導致 Amazon 的 EC2 實例 (instance) 被關閉，從而影響了 Webex、Okta、Splunk，及 BambooHR 等應用程式。雖然 AWS 報告停電僅持續了大約 20 分鐘，但一些客戶的服務和應用程式，需要長達 3 小時才能恢復正常。

3

企業面臨的另一個潛在重大資安隱憂，即是彈性化的雲環境，容易發生組態設定錯誤 (misconfiguration)。

相較於傳統的資料中心，雲環境的 IT 基礎設施具有以下特色：

- IT 設備種類繁雜，並且所有的資源都是使用者可以完全自行配置的，包括各式各樣的資源設定、資安政策、資訊資產，以及各種環環相扣的服務。開發人員和工程師可以根據需要，調配自己的 IT 基礎架構，且過程中無需通過資訊部門，或其他中間人協助。

- 依據前述「按需求的自助服務」的雲端運算特徵，雲環境的配置錯誤是可以被系統接受的。加上考慮到所有可用的不同類型的雲資源，以及它們可以組合在一起支援各種應用，實際上這些配置方式是接近無限的。

因此根據《2021 年雲安全狀況報告》，在過去一年中，36% 的企業因雲環境組態設定錯誤，而發生嚴重的雲環境資安漏洞，或資料外洩事件。Gartner 預計到 2023 年至少 99% 的雲環境資安事件，主要可以歸咎於客戶，而雲環境組態設定錯誤是主要的原因。

上述三個主要的雲端資安議題，可以進一步延伸到越權存取、不安全的 API、憑證意外洩露、雲環境缺乏能見度、錯誤的資料共享、雲客戶直接面對阻斷服務攻擊等潛在資安威脅，對企業的影響甚為嚴重。

資安風險分析

要探討雲端資安風險，OWASP 提出了十大雲端風險，OWASP 是 Open Web Application Security Project 的縮寫，對各領域提出了十大風險排名，最有名也是應用最廣泛的是 Web 資安風險的排名，故雲端風險也有其公信力，分列如下：

問責制和資料所有權
Accountability and Data Ownership

1

使用第三方存儲和傳輸資料會增加資安風險。這可能進一步導致公司資料的處理和維護方式缺乏透明度。

雲端服務商通常跨地理轄區營運，應該要求資料處理者和資料控制者對資料提供良好的保護，例如，歐盟的 GDPR 即有相關條例要求，亦即相關資安風險必須被重視並處理。

用戶身分聯合
User Identity Federation

2

數位身分是網路安全的關鍵之一，它控制重要資源與功能，例如對敏感資源的特權存取。因此雲端開發解決方案確保跨雲計算平台能正確識別用戶，對於企業安全至關重要。對於跨雲服務和應用程序的存取，通常會使用 SAML（安全斷言標記語言）；但是，如果執行不當，此解決方案會使攻擊者獲得未經授權的存取能力。

合規性
Regulatory Compliance

3

OWASP 指出了符合跨地域管轄時的合規性問題。例如，如果使用雲端服務的企業位於歐洲，但使用美國雲端服務商，則可能難以符合以歐盟為主的資料保護的合規性要求，反之亦然。

業務持續性和韌性
Business Continuity and Resiliency

4

將企業的 IT 基礎架構外包給第三方雲提供商，會增加業務持續性的資安風險，原因在於，IT 基礎架構超出了企業的控制範圍，當雲服務中斷，會對企業產生嚴重影響，例如，當亞馬遜當機 13 分鐘時，損失了大約 2 百多萬美元。

用戶隱私和資料二次使用
User Privacy and Secondary Usage of Data

5

一旦資料進入雲端領域，要控制資料的使用、修改就變得更加困難。社交媒體網站就是難以管理的最佳案例，通常資料會被默認為“全部共享”，也就失去了對資料的控制能力，也可能發生資料遭二次使用的狀況，也就是為了其他目的而將資料再次利用，這會將用戶的信息隱私置於危險之中，例如廣告分析、內容再利用等潛在隱私風險。

服務與資料整合
Service and Data Integration

6

由於可能有敏感資料透過 Internet 傳輸，因此保護傳輸中的資料，對於實施基於雲端的解決方案的企業尤其重要，若是資料傳輸缺乏安全保護，可能導致敏感資料曝露和公司訊息洩露。

多租戶和物理安全
Multi Tenancy and Physical Security

7

儘管基於雲端的解決方案具有強大的優勢，但如果託管在雲中的資源沒有做到確實的邏輯分隔，導致租戶資料保護不足，多租戶環境反而可能會導致安全風險。

事件分析和取證支持
Incident Analysis and Forensic Support

8

如果發生資料洩露，則必須了解如何識別和管理關鍵漏洞，以便盡可能快速有效地回應處理事件，而事件之後的分析過程需要收集日誌文件和相關資料以進行調查，但這在雲端環境中可能會變得複雜，因為多位置儲存，而且儲存位置是在不相關或屬於外部企業，導致在取證與恢復時會產生困難，或是無法執行相關程序。

基礎設施安全
Infrastructure Security

9

這項目涵蓋如何強化雲基礎設施的所有攻擊面向，它包括如何配置和安全區域規劃，以及確保使用預先建立的網路和應用程序協議，如未能落實基礎設施安全將帶來資安風險。

非生產環境下的曝露
Non-Production Environment Exposure

10

在開發應用軟體和部署階段相關的整個軟體生命週期中，必須考量相關風險，這包括進行開發和測試階段的測試環境，以及用來部署的環境，由於這些環境僅用於測試，所以在安全性上不一定足夠嚴格，導致帶來安全和隱私風險。

強化雲端資安

強化面向

面臨各種內外部的資安威脅，強化雲端資安成為企業必須正視的議題，可從以下三個方面來探討：

對外慎選雲服務供應商

從歷年發生的雲環境資安事件可以發現，雲服務供應商內部的惡意人員，特別是取得內部網路及敏感資源存取權限的人員，可以對客戶的資料造成致命的傷害。此外，負責管理客戶 IT 基礎設施及服務的 MSP 業者，也成為網路釣魚攻擊的目標。這些握有系統管理員或網域管理員權限的員工，一旦遭受駭客竊取其登入憑證，將引發災難性的後果。

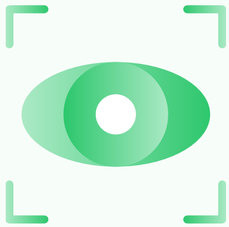
因此，企業一旦決定將核心業務所需要的 IT 基礎設施、重要機敏資料、關鍵服務等，交由雲服務供應商託管時，應慎選雲服務供應商，必要時利用嚴謹的使用者授權合約，及服務水準協議 (Service Level Agreement，SLA)，約束供應商 (及其員工)，是保障企業本身權益的重要手段。

由於內部人員的資安事件可能使大量高度敏感的資料面臨外洩風險，或導致客戶依賴的關鍵服務停擺，因此了解雲服務供應商，透過何種方法來偵測或診斷內部威脅，亦為評估雲服務供應商是否安全可靠的指標之一。

對內強化教育訓練

提升資安認知，降低雲環境組態設定錯誤而產生的風險，是強化雲環境安全的必要手段。對大多數的企業員工而言，構建安全的雲 IT 基礎設施或服務，其難度已超越了傳統資料中心的經驗。傳統資料中心的 IT 基礎設施，可以透過實體環境掌握各種安全配置，而雲端運算意味著使用者需要遠端透過 API、網路瀏覽器等介面，針對虛擬的雲環境進行資源分配及安全設定，且每個虛擬的部分 (例如：從 IT 基礎設施、網路、應用程式、資料等) 都需要安全保護。

因此對內強化教育訓練，讓所有部門參與並了解如何建構及使用雲環境，以及這可能對安全性產生何種影響，將是其中的關鍵。企業應根據行業最佳實踐基準 (例如 NIST SP 800-210)，進行評估，以了解既有雲環境及最佳實踐的差距，據以改善。另制定雲環境的業務連續性計畫 (Business Continuity Plan)，將有助於企業在雲環境出現問題時，可以在最短的時間內恢復一定程度的營運，這對高度依賴雲端運算的企業而言十分重要。



提升雲資料的可見性

知己知彼，是保護雲端資料安全的不二法門，這些包括：掌握儲存在雲環境的資料及其類型、雲端資料的使用者、有權存取雲端資料的使用者、雲環境使用者與誰共享資料、雲端資料的所在位置、存取和下載雲端資料的位置及設備等。

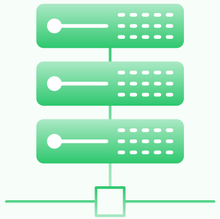
一旦企業清楚了解雲端資料的屬性，可透過資安控制措施，如資料外洩防護機制，防止機敏資料離開雲環境。定期進行雲端資料及服務的合規性審查、控制雲端資料的查閱權限，刪除資料共享連接，實現雲端資料自動加密等，皆是強化雲端資安的方法之一。

雲端資料保護機制

雲端存取安全中介 (cloud access security broker, CASB) 的目的，在於確保辦公室內裝置和雲端服務提供者間的網路資訊流通，可以符合企業的資料安全政策。完整的 CASB 解決方案，可透過本身「In the cloud, at access, on the device, and on the network」中的生命週期，確實保護資料安全，並兼顧個人隱私、易於使用，以及移動無礙。以下並利用前述 CASB 解決方案生命週期的四階段進一步說明：

In the cloud

CASB 可做為雲端資料安全的控制點，藉由 API 對雲端服務管制的反應，以及對所有使用 proxy 雲端服務的監控，保障雲端資料安全。此外，使用 CASB 解決方案，進行雲端加密的好處，在於它允許企業控制自己的加密金鑰，確保他人無法任意取得企業資訊。然而，使用 CASB 雲端加密也會影響部分應用程式功能，例如加密資料無法以 SaaS 應用伺服器處理，也難以被搜尋。



At access

與傳統 DLP 相同，CASB 解決方案需要提供可視性 (visibility)、身分辨別 (identity)、存取控制 (access control) 和資料保護 (data protection)：

可視性

CASB 解決方案可使跨越各雲端服務間的用戶行為和活動一目了然。典型的可視性涵蓋整個雲端部署，包含審計日誌與高階資料分析、報告和警示。

身分辨別

CASB 解決方案可協助在不同雲服務之間，以直接對照企業名錄驗證，或是透過第三方雲端身分辨識確認服務提供者，確保所有雲端應用程式使用單一身分庫 (single identity store)，甚至讓所使用的單一身分庫具有雲端身分辨識功能，減少帳號並且更有效的執行密碼政策。

存取控制

針對在什麼狀況與背景之下，誰被允許使用某項特定的雲端應用程式。存取控制政策應該基於：

- 企業中的群體和角色
- 裝置類型或作業系統
- 所在之地理區位

資料保護

如同前述的傳統 DLS 解決方案，所有 CASB 解決方案在資料保護上的第一步，就是辨明什麼是企業資料，並且能夠定義出模板或政策，將企業資料按照不同的風險或機敏程度分類。此外，企業本身要能夠依照應用程式、用戶或群體，以及資料，定義並判斷針對特定類別資料所應採取的行動。

On the device

CASB 解決方案不僅必須保護資料在雲端的儲存和存取，也要保障雲端資料在進行使用的機器上之安全，包括：

- 企業機敏資料用戶端加密
- 選擇性地從移動裝置上抹除雲端資料
- 資料追蹤與建立資料指紋
- 執行基本的裝置安全政策

OWASP 雲端資安 10 大議題防護

要探討雲端資安風險，OWASP 提出了十大雲端風險，OWASP 是 Open Web Application Security Project 的縮寫，對各領域提出了十大風險排名，最有名也是應用最廣泛的是 Web 資安風險的排名，故雲端風險也有其公信力，分列如下 :

1

問責制和資料所有權
Accountability and Data Ownership

為了減輕責任和資料所有權的問題，建議企業和雲端服務商對資料的存儲方式進行深入的瞭解，以及盡可能提高透明度，此外，企業應該知道使用了哪些安全機制來保護資料，以及雲端服務商的備份和恢復機制。

2

用戶身分聯合
User Identity Federation

應該確保在雲服務上，對用戶身分識別的方法與企業的政策和標準是一致的，並建立資源的存取模式，這有助於管理對特權資源的存取安全。

3

合規性
Regulatory Compliance

為避免違反合規性相關的法律，企業和雲端服務商之間，應完全透明地了解其資料的儲存位置和適用的司法管轄區，並確保雲端服務商對託管資料適用哪些法律有充分的了解。

4

業務連續性和彈性
Business Continuity and Resiliency

企業應與雲端服務商協調，確保當緊急情況時，已經有制定可執行的災難恢復和業務連續性應變計畫。

5

用戶隱私和資料二次使用
User Privacy and Secondary Usage of Dat

用戶資料的使用方式要有清楚的了解，並且制定資料使用和隱私保護政策，並與雲端服務商進行協調，確保政策實施落實，加強對用戶私人訊息的保護。

6

服務與資料整合
Service and Data Integration

強制使用強力的加密協議進行資料傳輸，例如 SSL/TLS，有助於保護這些訊息的機密性。

7

多租戶和物理安全
Multi Tenancy and Physical

雲端服務商應對多租戶環境強制執行適當的邏輯分離，並隔離每個租戶的基礎架構。從企業角度，應確保瞭解資料儲存方式和位置，以及雲端提供商為防止資料洩露而採取的措施。

8

事件分析和取證支持
Incident Analysis and Forensic Support

企業應與其雲端服務商進行協調，以分析雲端的事件日誌是如何生成和儲存，並瞭解當事件發生如何進行取證與恢復動作。

9

基礎設施安全
Infrastructure Security

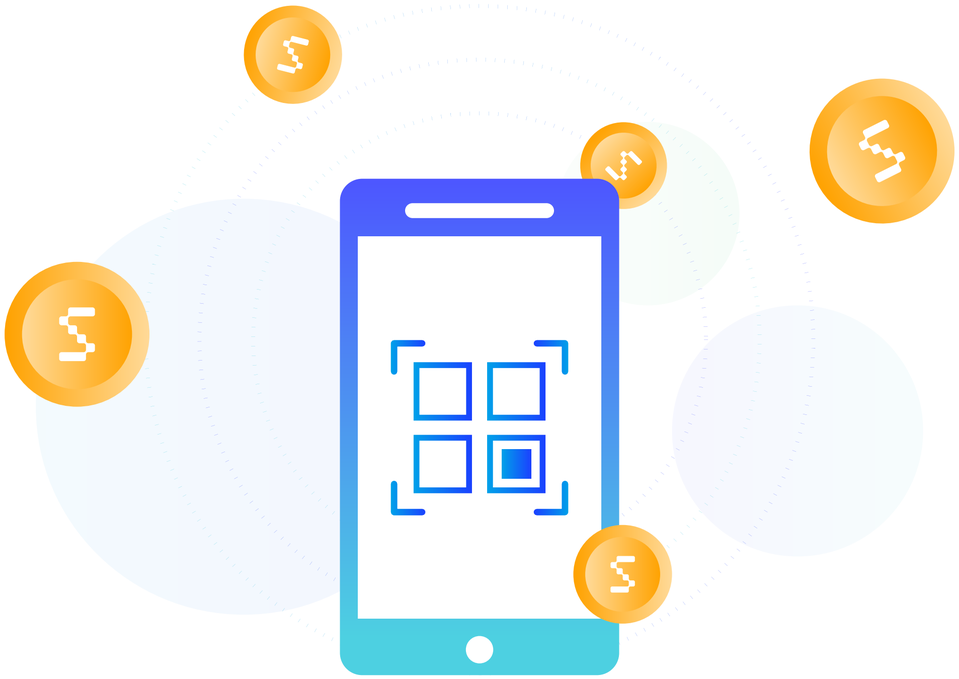
一般常見的安全措施皆適用於基礎設施安全，例如進行漏洞評估和軟體更新修補，建議可參考更多漏洞管理措施。

10

非生產環境下的曝露
Non-Production Environment Exposure

應避免將敏感資料儲存在非正式的產品環境中，並確保對資料的存取受到限制，並有相應的保護。

2.2.3
行動支付資安與案例研析



行動支付簡介

行動支付為我國政府近年來大力推動的國家發展政策之一，為使行動支付更為普及，自 2016 年起相關部會陸續修訂與鬆綁法令，並推出眾多行動支付應用，以建立友善的行動支付環境。在政府及民間業者的共同努力下，行動支付使用率也逐年提升，根據金融監督管理委員會統計，截至 2021 年 10 月底，國內行動支付使用者已達 1,581 萬人，預計未來還會持續成長。

行動支付主打交易、轉帳免現金，解決民眾攜帶現金可能面臨遺失或遭搶奪等風險，卻難杜絕有心人士利用 APP 漏洞、竄改或覆蓋 QR code 誘導民眾開啟惡意連結等方式進行詐騙。行動支付也絕非如宣傳中的安全，如不慎遺失手機或遭駭客盜刷時恐造成重大損失。此外，消費習性易被掌握而遭廣告騷擾，因此行動支付的相關法規訂定、安全交易系統的建置及使用者安全已成為刻不容緩的全球議題。

行動支付的種類與交易流程

行動支付的概念，為任何行動載具（如手機）以非現金方式進行付款交易之行為。交易方式主要又可分為兩種，一種是使用 NFC (Near Field Communication，近場通訊）功能進行的「感應支付」，以 Apple Pay、Google Pay 及 Samsung Pay 為國際三大主流，其特色是交易時是利用行動裝置內建的 NFC 功能進行感應傳輸，故不需要啟用網路，行動裝置僅為信用卡的載體。另一種則為透過 QR Code 掃描方式的「掃碼支付」，交易時需啟用網路，但因不限定廠牌手機是否具備 NFC 通訊功能，使用門檻較低，故配合的商家最為廣泛，如夜市或手搖茶飲店常見的街口支付或 Line Pay 等。

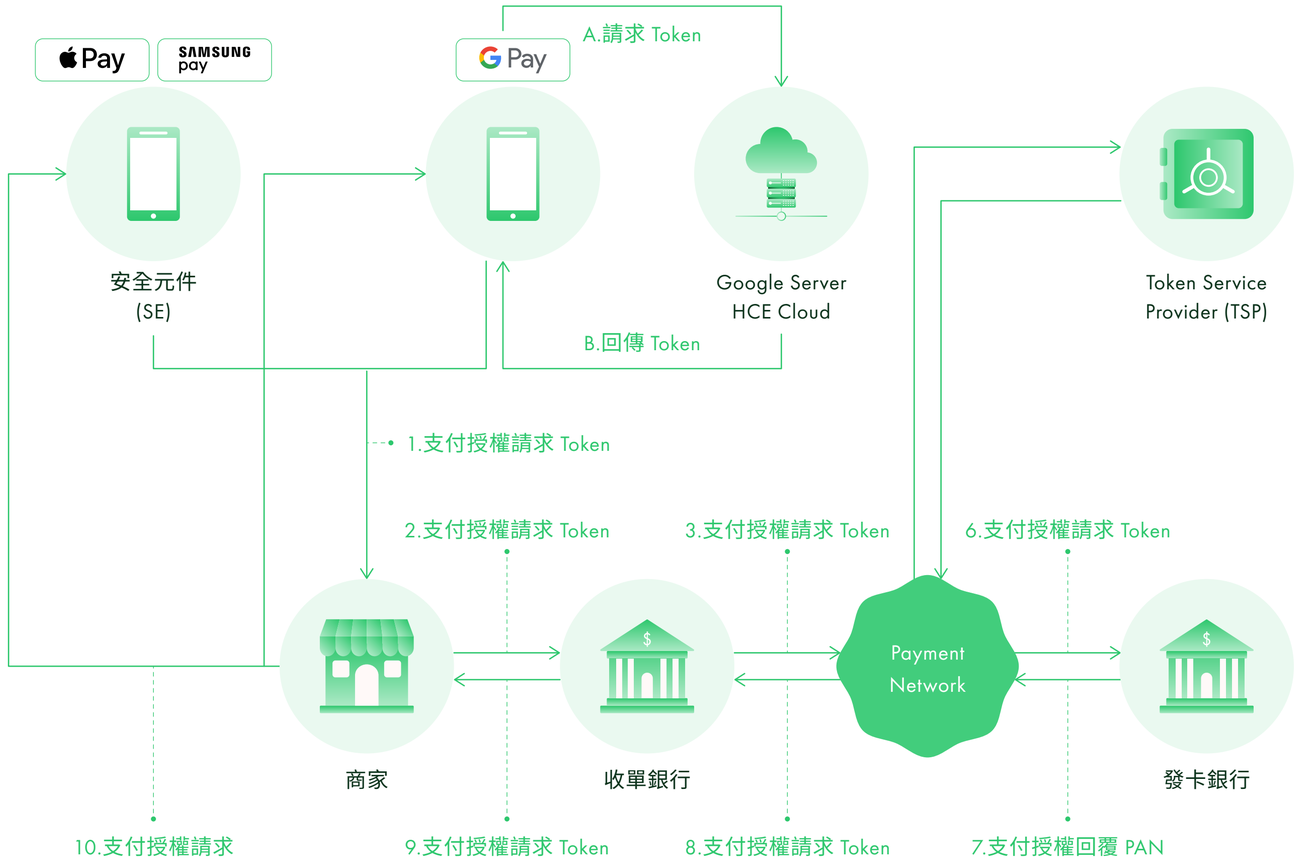
感應支付

感應支付主要之技術採用近距離無線通訊 (NFC) 與代碼化技術 (Tokenization)，透過 TSP 將卡號轉換成代碼 (Token)，降低因卡號洩漏而導致被盜刷的風險，並利用手機具備硬體的安全元件 (Secure Element，SE)，儲存代碼及金鑰，支付流程詳見圖 1。此類代表性的支付 APP 如 Apple Pay、Samsung Pay 及 Google Pay。

在 Apple 與 Samsung 支付流程中，消費者透過行動支付安全元件 (SE)，將用戶資料 (Primary Account Number, PAN) 轉成支付代碼 (Token)，透過感應式掃描裝置傳送支付請求經由商家 (1)、收單銀行 (2)、Payment Network(3) 至代碼服務提供商 (Token Service Provider, TSP)(4) 轉回 PAN(5)，提供發卡銀行 (Issuer) 處理持卡人認證程序 (6)，並將支付授權回覆回傳至 Payment Network(7)，再將 PAN 轉回代碼 (Token) 後，傳送至收單銀行 (8)、商家 (9) 與消費者手機 (10)。

Google Pay 是由主機卡模擬 (Host Card Emulation，HCE) Cloud 搭配手機支付 APP 來模擬 SE，代碼與金鑰儲存在 Google Pay APP 中，但金鑰有使用限制，需從 HCE Cloud 下載更新。

圖 10：感應支付流程



資料來源：TWCERT/CC 整理

QR Code 掃描支付

掃描支付主要技術以掃描 QR Code 方式進行支付，由於不需要特定廠牌手機與通訊功能，目前國內業者與配合的商家最多。流程如圖 11 所示。

在 QR Code 支付流程中，QR Code 可分為商家掃描消費者 QR Code 的被掃 (A1)，與消費者掃描商家 QR Code 的主掃模式 (B1)，支付授權請求被傳送至支付服務供應商 (A2、B2)、收單銀行 (3)、Payment Network(4)、發卡銀行 (5) 進行驗證與支付處理，最後將支付請求回覆回傳至商家與消費者手機 (6-A9/B9)。

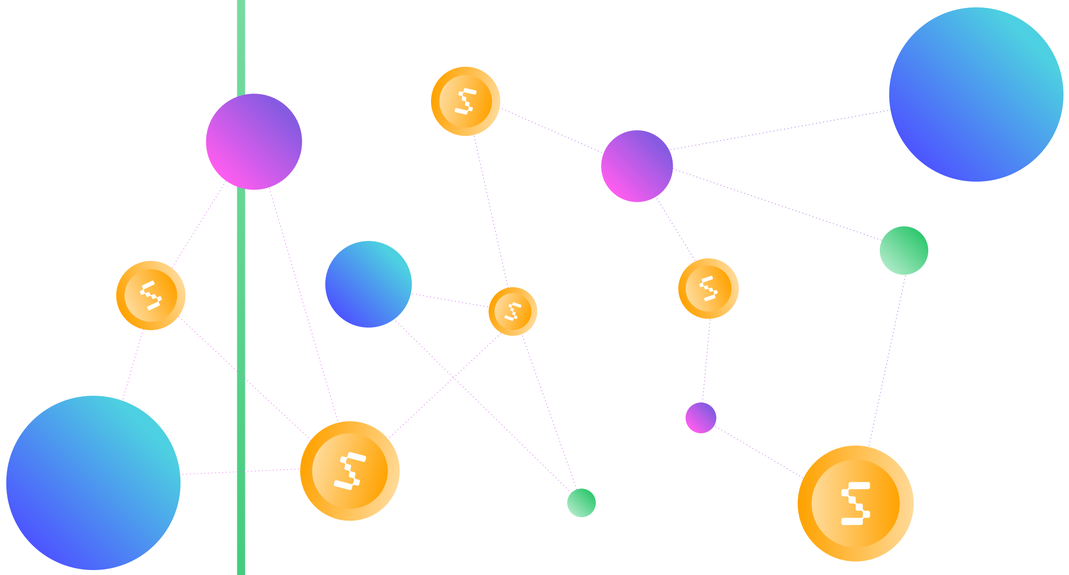
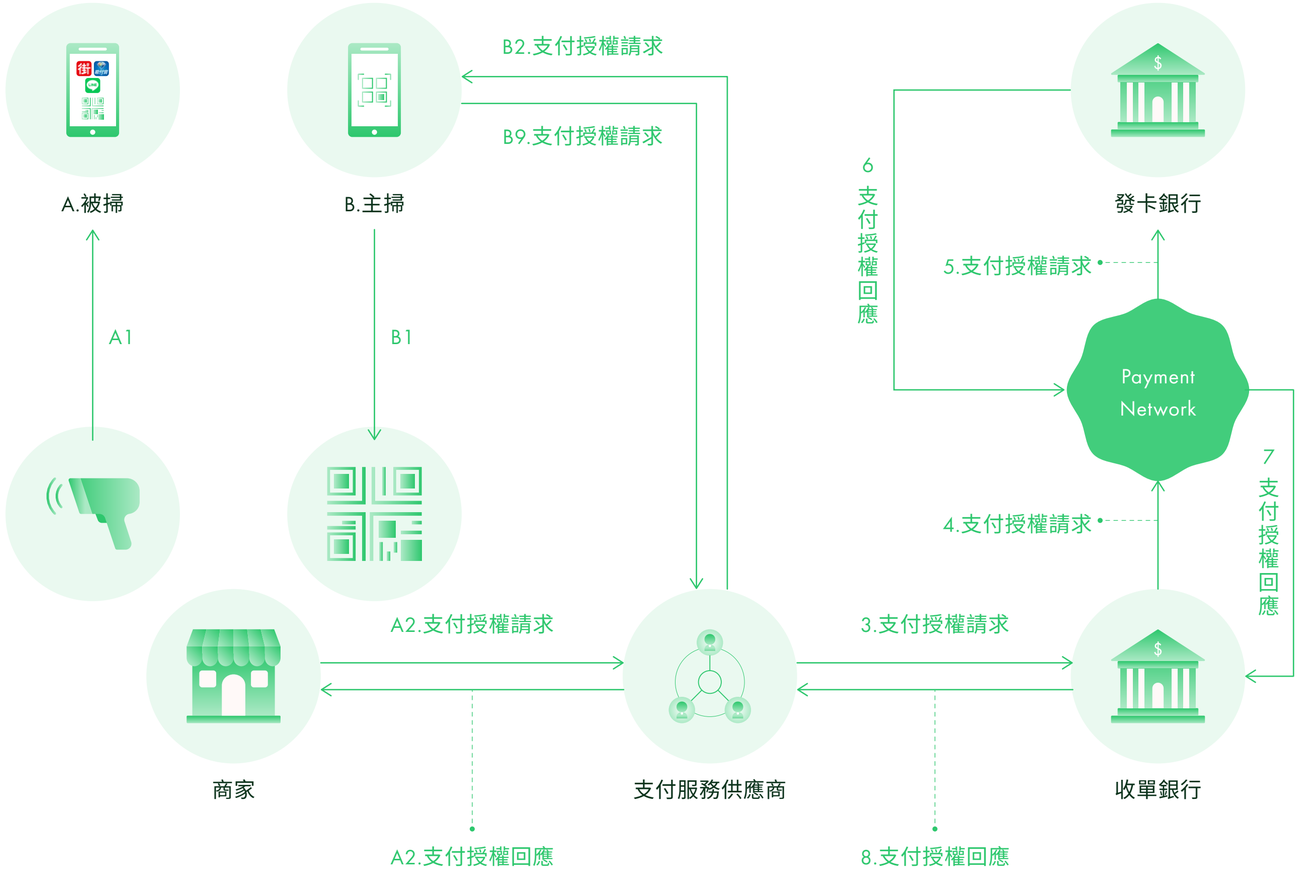


圖 11：掃碼支付流程



資料來源：TWCERT/CC 整理

國內行動支付現況

除了較常見的 LINE Pay、街口支付等，國內各大通路也陸續推出自己的專用錢包 (表 1)，但僅限定在自家通路使用。此類支付的架構圖如圖 3 所示。其交易的流程圖與一般 QR Code 支付類似，差異點為交易通訊皆會經過商家中繼 Server，如同收單行的角色，必須包含處理金流服務的功能，商家也需要自行維護該伺服器及遵循相關資安規範與法規。

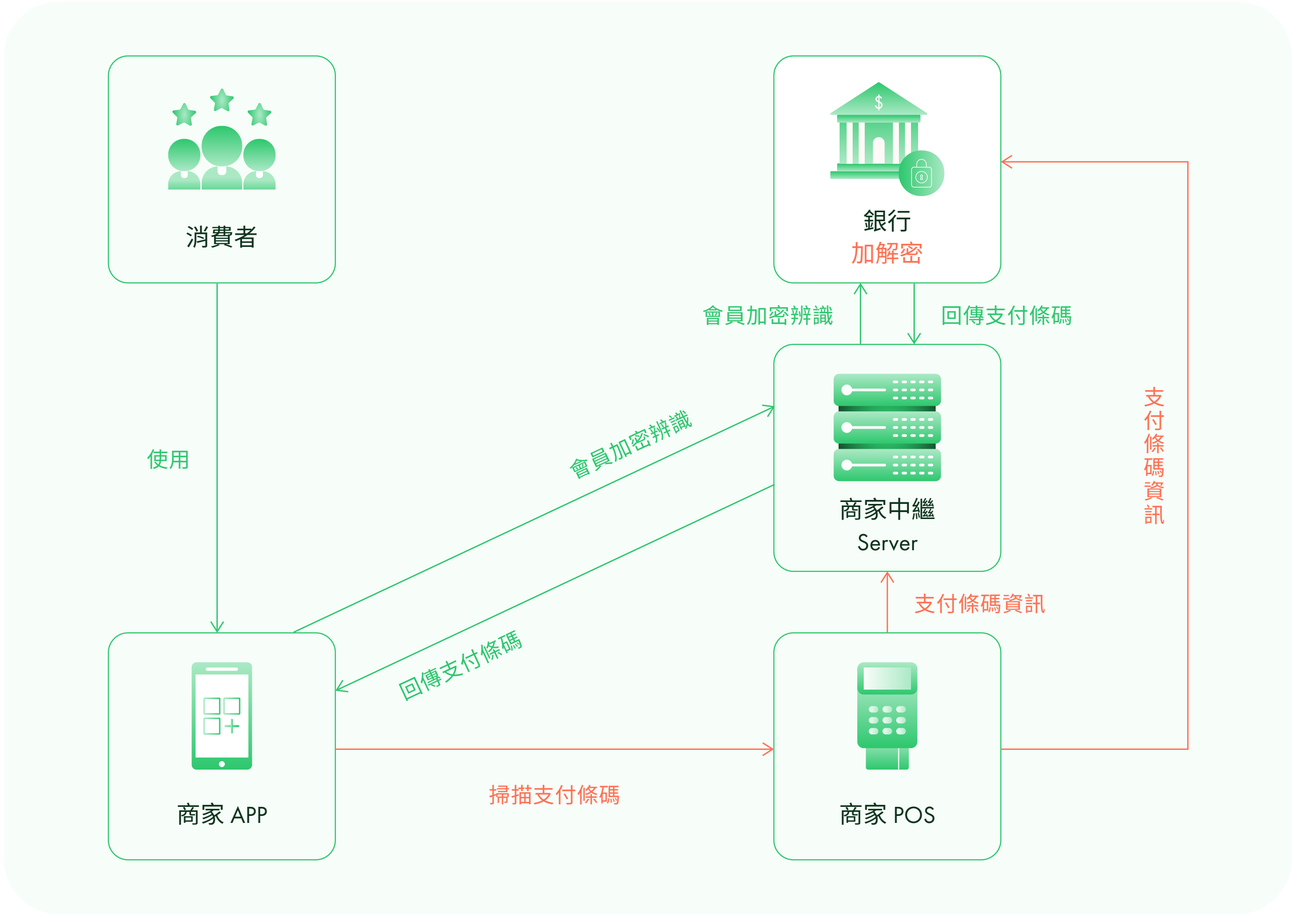
表 1、國內電子錢包、支付種類

產業	專用錢包 / 支付 APP
百貨業	微風 Breeze Pay、新光三越 skm pay
零售業	全聯 PX Pay、全家 My FamiPay、屈臣氏 Watsons Pay、萊爾富 Hi Pay、7-11 open 錢包、icashPay
餐飲業	85 Café APP、摩斯 MOS Order、Cama Pay

資料來源 : TWCERT/CC 整理

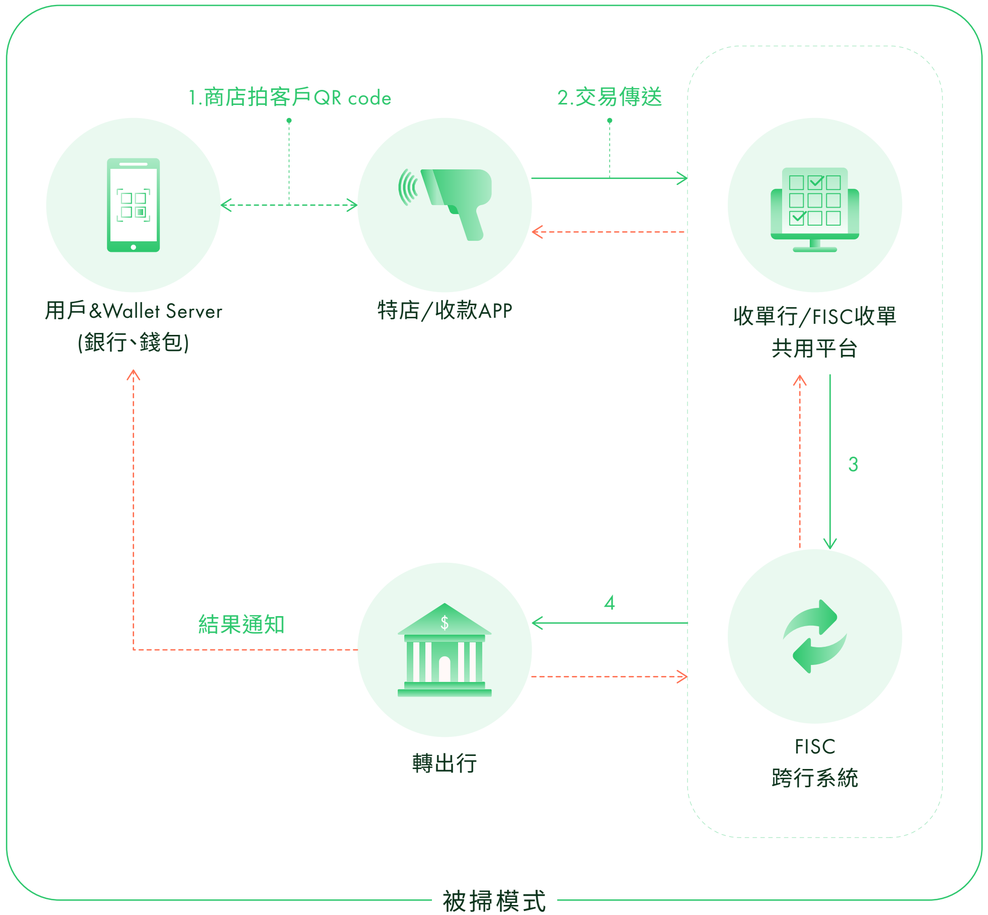
隨著我國多家金融機構、行動支付及第三方支付業者推出多達數十種 QR Code 支付 (如 Pi 行動錢包、街口支付、LinePay 等)，QR Code 缺乏整合性，導致各種支付之間無法互通，間接影響消費者與商家的使用意願。因此，「公股事業金融科技研發成果整合平台」自 2016 年起制定「台灣 Pay QR Code 共通支付」標準，並於 2017 年推出「台灣 Pay QR Code 共通支付」。除推動統一國內 QR Code 行動支付規格，架構設計上更強化交易安控機制，每筆交易皆會即時傳輸至財金公司進行特店的檢核 (圖 4、5 紅框處)，有效防止 QR Code 遭竄改或偽造，大幅提升交易之安全性。使用者包含台灣 Pay 用戶以及國內金融機構之行動網銀用戶，經由行動網銀 APP 使用台灣 Pay。未來我國政府亦將持續致力於國內支付統一。

圖 12：國內行動支付架構圖



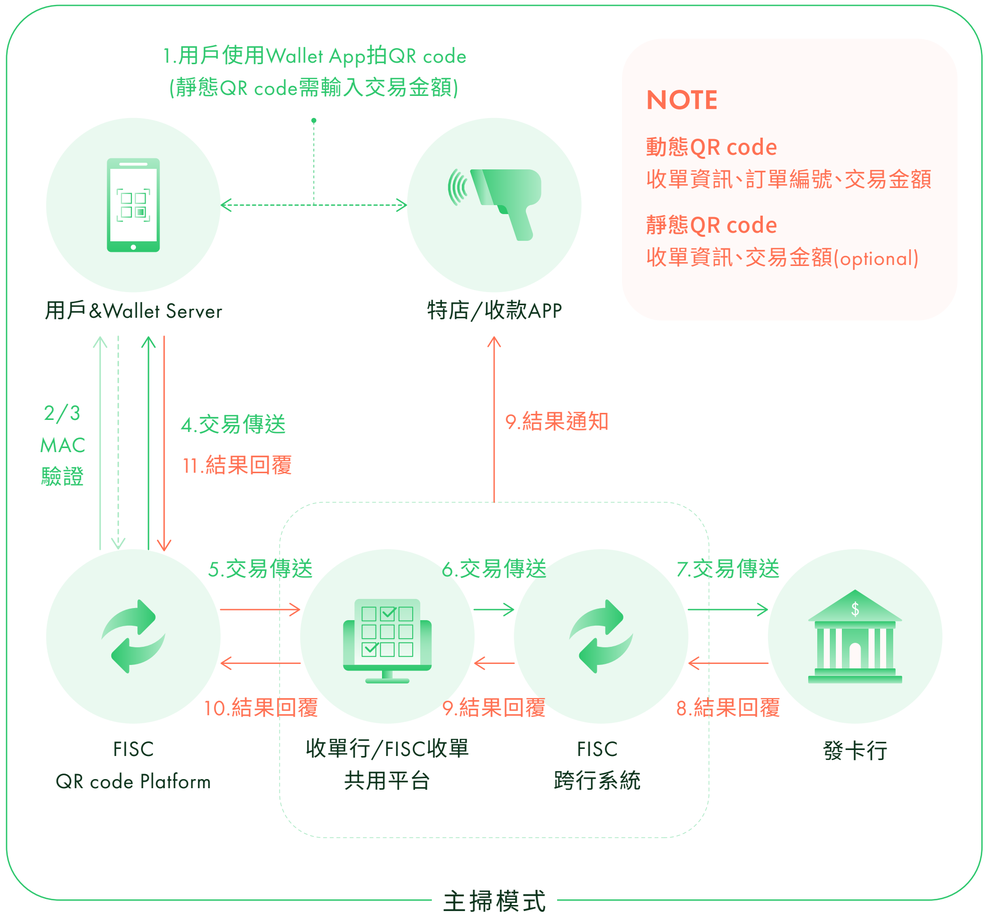
資料來源 : TWCERT/CC 整理

圖 13：台灣 PAY QR Code 共通支付被掃流程圖



資料來源：金融監督管理委員會

圖 14：台灣 Pay QR Code 共通支付主掃流程



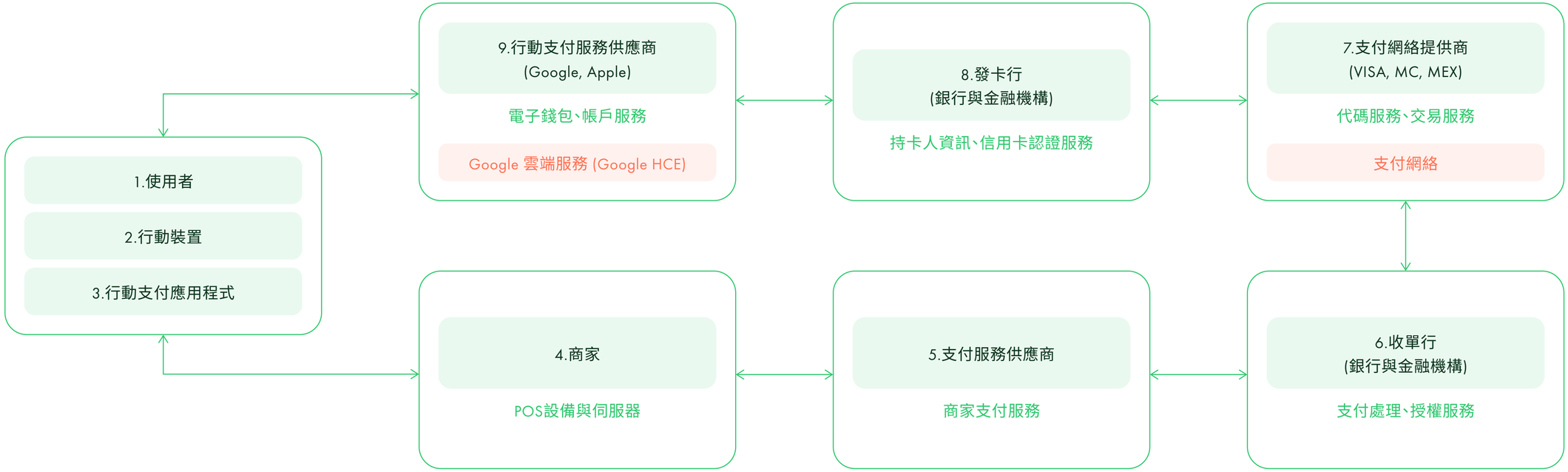
資料來源：金融監督管理委員會

行動支付的威脅分析

行動支付的安全廣泛涉及使用者、商家、支付服務單位、卡務 / 帳務單位等，如有任一環節發生問題，則嚴重影響整體行動支付安全，因此威脅分析應全面性地納入各個環節。根據歐盟網路和資訊保安局 (ENISA) 提出的行動安全指南，行動支付的主要角色分類如圖 6 所示。以「台灣 Pay QR Code 共通支付」為例，「用戶錢包」可對應到 「使用者、行動裝置、行動支付應用程式」模組 (1-3)、「特店 / 收款 APP 」、 「FISC QR Code 共用平台」、「FISC 收單共用平台」、「FISC 跨行系統」、「發卡行」可各別對應至「商家」(4)、「支付服務供應商」(5)、「收單行」(6)、「支付網絡供應商」(7) 及「發卡行」(8)。Google、Apple 等感應式支付模組則對應到「行動支付服務供應商」(9)。

本章將上述之威脅模組歸納成三大類型，分別為使用者、行動裝置及支付應用程式的「行動裝置端」，支付服務供應商、收單行、商家、支付網絡提供商、發卡行、行動支付服務供應商的「服務端」，及各模組之間通訊的「傳輸端」。以下根據各別類型進行威脅面向探討與防護建議。

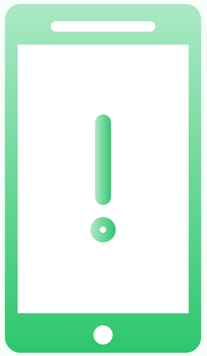
圖 15：行動支付威脅模組



資料來源 : TWCERT/CC 整理

1

行動裝置端威脅



釣魚攻擊

攻擊者可透過如電話、電子郵件、簡訊等通訊管道，結合如社群媒體、搜索引擎等公開資訊進行釣魚攻擊。竊取僅有受害者知道的信用卡、個資等機敏資訊，並透過盜刷信用卡、販賣信用卡認證資訊 (如 PAN、CVV、卡片到期日期) 獲利，或是冒充受害者身分進行其他非法行為。

惡意程式感染

攻擊者可透過社交工程郵件、釣魚郵件等方式，誘導受害者開啟郵件的惡意附檔或是開啟惡意連結將惡意程式植入受害者設備。

攻擊者可透過植入後門程式 Rootkit，直接監控或變更受害者支付 API 呼叫功能的變數，如竄改支付金額等。

手機竊盜與未經授權存取

攻擊者如取得受害者行動設備，可透過商用或開源鑑識工具破解行動設備 (Jailbreak)，進而取得作業系統的完全控制，竊取存於手機的機敏資訊。

在 HCE 的架構下，通訊皆會經過 Android OS，所以行動設備一旦遭受破解 (Rooting)，交易資訊就有可能外洩，如不慎感染惡意程式，則支付身分驗證等機敏資訊也會相對容易被竊取。

行動設備 OS 的存取權限可透過使用者授權賦予應用程式，但此舉可能有外洩行動設備儲存之機敏資訊的潛在風險，或是被其他應用程式利用進行存取提權。

逆向工程與應用程式源碼邏輯曝露

攻擊者可透過逆向工程反編譯支付 APK 檔，獲取應用程式邏輯或是其他可使用於攻擊行為的重要資訊，如硬編輯的密碼 (hardcoded passwords)、加密金鑰等。

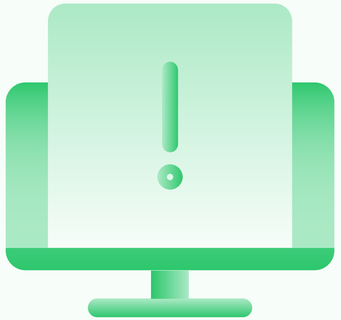
支付應用程式竄改

攻擊者可能透過下載行動支付的官方應用程式，植入惡意程式碼，封裝後再上傳至 APP 下載平台，導致使用者下載使用竄改後的惡意支付程式。

支付應用程式竄改

攻擊者可能透過下載行動支付的官方應用程式，植入惡意程式碼，封裝後再上傳至 APP 下載平台，導致使用者下載使用竄改後的惡意支付程式。

服務端威脅



漏洞利用與系統入侵

收單行伺服器與系統如存在不安全的系統配置或是安全性漏洞，可能讓攻擊者植入後門程式或遠端存取工具 (RAT)，達成系統入侵目的。

代碼化服務供應商 (TSP) 如存在安全性漏洞，可讓攻擊者竊取交易中的支付者 (PAN) 與信用卡資訊。另外也可藉由入侵代碼化服務伺服器，竊取代碼對照表 (token look-up table)，以利後續對照代碼所對應的 PAN、CVV、有效日期等機敏資訊。

機敏資訊外洩

發卡行的信用卡資料庫通常皆遵守嚴謹的安全規範，但攻擊者仍可能透過社交工程郵件攻擊取得員工存取資料庫權限，或是透過植入 RAT 等 APT 攻擊方式，將信用卡機敏資訊與資料庫加密金鑰回傳給攻擊者 C2，造成機敏資訊外洩。

第三方支付平台存有未代碼化的卡片完整資訊、掌握個資、卡號及交易紀錄、HCE 掌握卡號與交易紀錄、Apple Server 掌握卡號，如有遭受入侵，則有大量機敏資訊洩漏疑慮。

傳輸端威脅

不安全的連線

攻擊者可能利用商家交易系統的資安脆弱點，如未使用防火牆、安全性漏洞、不安全的設定、未使用 SSL/TSL 加密傳輸等，進行中間人攻擊，例如受害者連結不安全的 WiFi 熱點 (如網咖等)，或是連結攻擊者配置的假基地台 (AP)，導向假認證釣魚網頁，竊取使用者身分驗證資訊。

收單行、發卡行、支付 APP 及支付服務供應商之間的不安全連線 (如未使用 SSL/TSL、VPN)，可能導致攻擊者進行中間人攻擊，竊取支付的機敏資訊。

Relay 攻擊

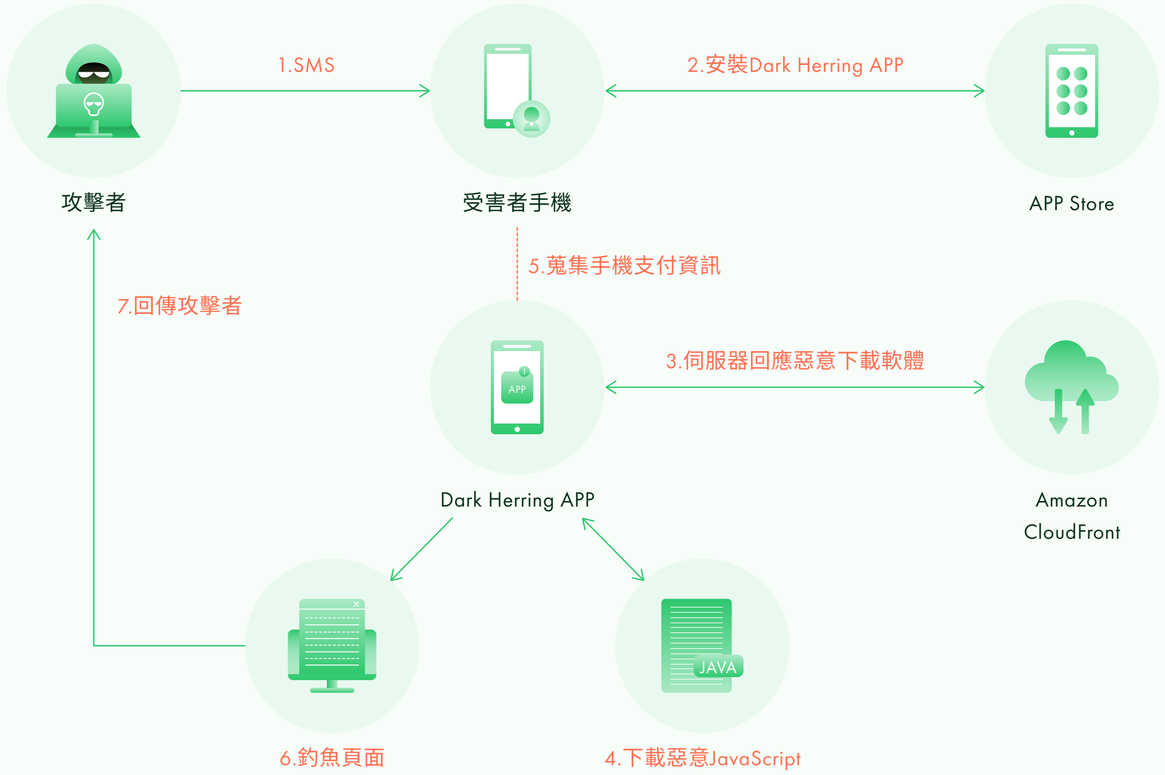
NFC POS 設備如遭攻擊者植入 Relay 軟體，可將行動支付 SE 與卡片模擬功能之間的請求與回應傳送至遠端攻擊者，用於未經授權的付款行為。

國內外行動支付威脅案例

惡意程式威脅

Android 智慧手機作業系統提供用戶保持一定的自由度，可以選擇安裝 Google Play Store 以外的第三方 APK 下載平台的安裝檔。除此之外，如因手機生產等原因未獲 Google 授權使用 Google Mobile Services，仍可建立自己的 APP Store，如受美國商務部禁令限制的華為手機，所推出的 AppGallery。這種第三方 APK 下載平台雖然提供用戶更多的 APP 下載來源選擇，但卻很難確保所提供的 APP 安全性。而所提供的行動支付、金融相關的 APP，也很有可能會夾帶惡意程式。台灣電腦網路危機處理暨協調中心 (TWCERT/CC)，於 2021 年間的官網通報中，有近四成的金融機構通報「第三方 APK 下載平台未經授權提供金融 APP 下載」的案件，這些金融 APP 因具有高度資安風險而受到國內銀行業高度重視。攻擊者極可能透過下載官方應用程式，植入惡意程式封裝後再上傳至第三方 APP 下載平台，導致使用者下載使用含有惡意程式的金融 APP，遭竊取消費者身分驗證資訊、信用卡交易驗證等機敏資訊，進而被盜用，造成財務損失。

圖 16：Dark Herring 攻擊流程



資料來源：TWCERT/CC 整理

2021 年 10 月，資安廠商 Zimperium[5] 揭露行動付費詐騙 APP，名為 Dark Herring，全球有包含台灣、日本、美國等 70 多個國家，多達 1.05 億支裝置安裝、使用此程式受害。攻擊流程如圖 16 所示。攻擊者透過簡訊 (1) 引誘行動設備用戶安裝 Dark Herring APP(2)，這些程式中並不含有惡意程式碼，而是含有硬編輯的加密字串，指向 Amazon CloudFront 的 URL 位置，當 APP 與該位置通訊時，伺服器會回傳另一下載連結 (3)，提供 APP 下載惡意 JavaScript 至行動裝置 (4)，伺服器回應如圖 17 所示。此 JavaScript 會感染行動裝置，並收集行動裝置使用者的支付相關資訊 (5)，如語言、國家與地區及所對應的電信商直接結算功能 (Direct Carrier Billing，DCB)。最後 APP 顯示客制化的釣魚網頁 (6) 如圖 18 所示。以誘導使用者輸入電話號碼以取得 OTP 驗證碼的方式，竊取行動裝置電話號碼，並將資訊回傳給攻擊者。目前 Google Play 已移除所有 Dark Herring 相關 APP，但仍可於第三方 APK 下載平台取得。這樣的資安威脅，也凸顯側載風險及行動裝置端軟體安全的重要性。

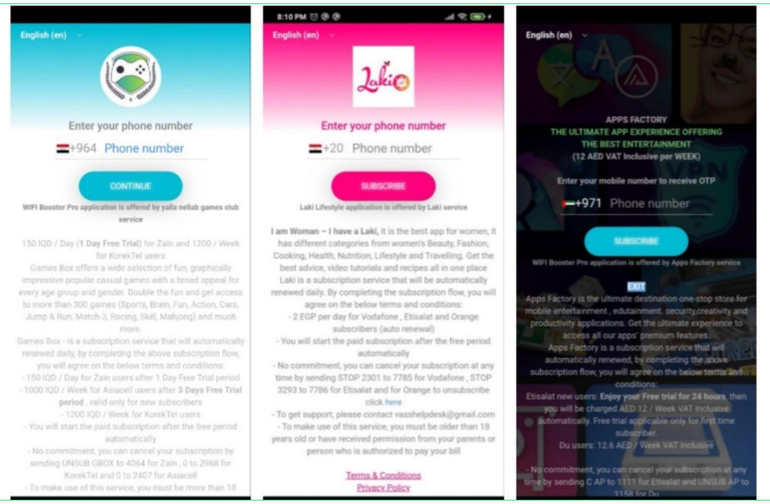
圖 17：Dark Herring 伺服器回傳之惡意 Javascript 下載連結

```
HTTP/2 200 OK
Content-Type: text/html
Content-Length: 6041
Date: Thu, 11 Nov 2021 13:29:27 GMT
Last-Modified: Thu, 04 Nov 2021 12:11:28 GMT
X-Amz-Version-Id: KLBbTG.PZgs08J9iaULWvSEluKO2puMU
Etag: "ce8746e3fdc95ae734bbd83e92fe726a"
Server: AmazonS3
X-Cache: Miss from cloudfront
Via: 1.1 ac28147bf6a75debb0811f62b6224e6f.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: IAD89-C3
X-Amz-Cf-Id: L4tO9_W-EN6PkUJqvPmyB_CKPSMEkVEfYaMo2fmXc8L9lz860yWy4w==

<!doctype html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>
      Appsdk
    </title>
    <base href="/">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link rel="icon" type="image/x-icon" href="favicon.ico">
    <script src="https://[redacted].amazonaws.com/asstes/JS/jquery.min.js"
    </script>
    <script src="https://[redacted].amazonaws.com/asstes/JS/bootstrap.min.
    </script>
    <link rel="stylesheet" href="https://[redacted].amazonaws.com/asstes/C
    <link rel="stylesheet" href="https://[redacted].amazonaws.com/asstes/C
    <link rel="stylesheet" href="https://[redacted].amazonaws.com/asstes/C
```

資料來源：Zimerium

圖 18：Dark Herring 用來取得使用者電話號碼的釣魚畫面

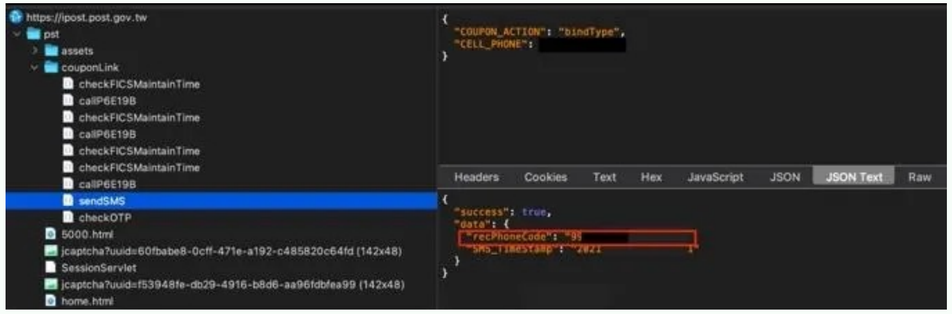


資料來源：Zimerium

不安全的資料傳輸

國內郵政機構在 2021 年 9 月開放五倍卷數位綁定時，因開發團隊將 OTP 身分驗證碼以明碼方式回傳至瀏覽器當中，造成 OTP 驗證碼可透過瀏覽器 F12 的開發者工具直接檢視，如圖 10 所示，申請者無須經過手機雙重認證即可透過這個漏洞成功綁定五倍券。OTP 如可直接從瀏覽器取得，將可避開經由使用者的行動裝置進行身分驗證的程序，可能產生被冒用帳號的風險。若有心人士可利用 OTP 驗證的系統設計疏失，而得以登入他人的帳號，並連接至網銀帳號或是社交軟體帳號等，恐怕就造成如財物損失或個資外洩等重大的資安風險。所幸，本次郵政機構綁定五倍券的系統設計瑕疵，並無被連接至後端網路系統的案例。

圖 19：含有 OTP 驗證碼的開發者工具頁面



資料來源：TechOrange

安全設計不足

2021 年，Apple Pay 被揭露安全性漏洞，當啟用 Express Transit/Travel 功能時，駭客可繞過 Apple 的安全機制，盜刷使用者的 Visa 信用卡。Express Transit 功能為在使用者不需與之互動，甚至不必解鎖手機的狀況下就能進行支付。此攻擊方式需要一 Reader emulator (Proxymark) 假冒成正常讀卡機，與一支手機當作卡片模擬器。

攻擊流程如下：

a、攻擊者透過 Reader 模擬器 (Proxymark) 假冒成讀卡機，傳輸 “magic byte” 至 iPhone 設備，讓 iPhone 支付系統以為收到支付交易請求

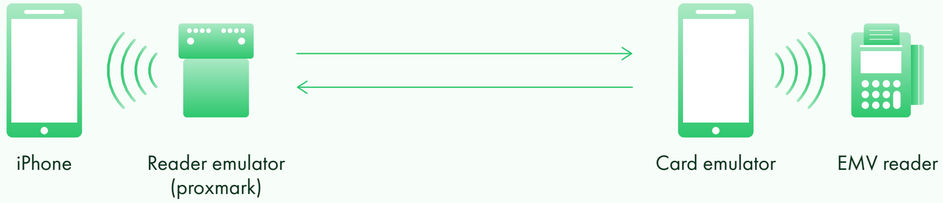
b、錄取 iPhone 設備回應，更改離線資料認證 (Offline Data Authentication, ODA) flag 至 “true”

c、遞交竄改後的回應至駭客手機

d、模擬卡片通訊傳送至 EMV 支付設備進行盜刷

此攻擊模式為典型的中間人 (Man-in-the-middle) 重放與中繼攻擊，如圖 11 所示。目前 Apple 與 Visa 皆未修補該漏洞，因此使用者應避免指定 VISA 信用卡作為 Express Transit 的支付工具，以保障自身權益。

圖 20：Apple 手機中間人攻擊示意圖



資料來源：Bleepingcomputer

日本超商 7-11 於 2019 年 7 月 1 日推出行動支付系統「7pay」，因其應用程式含有資安漏洞，導致在隔日就陸續傳出大量盜刷的災情。攻擊者可以透過已知的受害者電子信箱，即可重設帳戶密碼，取得帳戶的控制操作權限。

7pay 支付系統的密碼設定條件中所隱藏的安全問題如下：

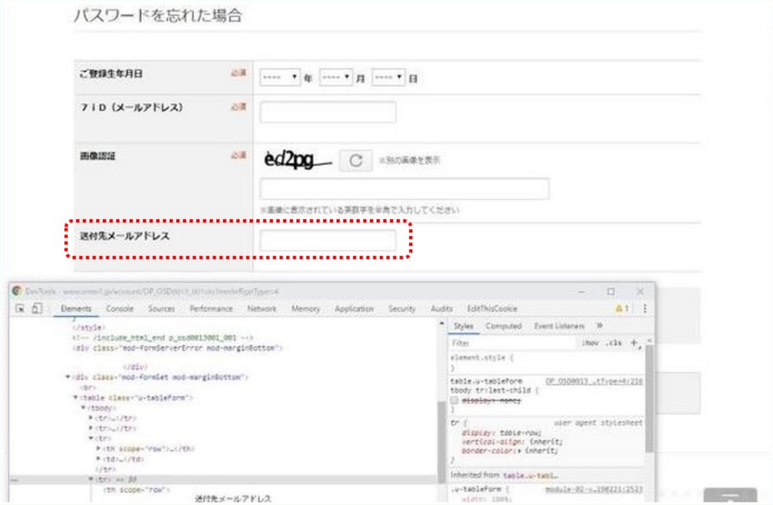
- 7pay 以電子信箱作為帳號
- 登入密碼時，無設定錯誤次數上限
- 用戶若想找回或更改密碼，僅需註冊時填寫的「生日」
- 申請註冊時，出生年月日為非必填選項，若用戶未填，系統會自動設定成 2019 年 1 月 1 日
- 想重設或找回密碼時，即使將生日填錯，也沒有錯誤次數的上限
- 找回或重設的密碼，可以填寫另一個新的電子信箱接收新密碼，不一定要使用註冊時填寫的電子信箱
- 未採用雙因子身分驗證機制

安全漏洞利用流程如下：

1. 在 7-pay 密碼重置頁面 (如圖 21 所示)，以已知受害者電子郵件作為帳號 (7iD)
2. 以已知受害者出生年月日、系統預設出生年月日、或是暴力破解 7-pay 帳戶出生年月日資訊
3. 填入攻擊者信箱接收新密碼 (圖 #)
4. 登入 7-pay 受害者帳號進行盜刷

此資安漏洞一個月餘仍無法修補解決，因此在 2019 年 9 月底停止服務。此事件有 808 名受害者，被盜刷金額折合新台幣約一千萬元的損失。7pay 社長曾表示，「7pay」支付服務未導入身分雙因子認證機制，是想盡可能先降低使用者門檻，之後再加強資安防護，此事件結果顯示這是不適當的安全設計。

圖 21：7-pay 密碼重置必填欄位與可收取新密碼的電子郵件欄位 (紅框處)



資料來源：日經

資料外洩

LinePay 於 2021 年 12 月發生資料外洩事件，日本官方坦言共有約 13 萬筆用戶資料被誤傳至 GitHub，其中亦影響台灣約七萬多用戶。遭外洩的資料中包含消費者交易日期、金額、帳戶名與店家識別碼，有心人士可透過分析得知用戶資料，但並未直接透露消費者姓名、電話、住址、信用卡及銀行等敏感資訊。

行動支付供應商通常會記錄消費者交易資訊，作為市場行銷等商業用途，但也因掌握龐大消費者資料，如因資安疏失導致資料外洩，可能被濫用於社交工程詐騙攻擊，危害消費者利益。

行動支付的安全防護

消費者以及商家在各個行動支付交易環節上，應意識到使用行動支付服務所可能衍生的資安風險。本段簡述與行動支付相關的行動設備端、傳輸端、服務端的最低資安建議措施及相關安全規範。

詳細的防護措施、漏洞風險管理請參考 ENISA 的行動支付與電子錢包安全指南。

各面向的安全建議

行動設備端 / 使用者端

i. 即時 / 定期更新行動設備的作業系統、應用程式，以降低安全性弱點遭受利用之風險。
ii. 使用行動支付時，應避免使用如公用 WiFi 熱點等不安全的網絡，以降低通訊被攔截的風險。
iii. 身分驗證應盡可能採用雙重因子認證，生物認證或強密碼 PIN/ 圖形認證。
iv. 確保行動裝置遺失時可遠端清除設備資料。
v. 不啟動小額支付功能。
vi. 不破解手機、不安裝非官方的 APP。
vii. 不隨意賦予 APP 非必要的存取權限。

傳輸端

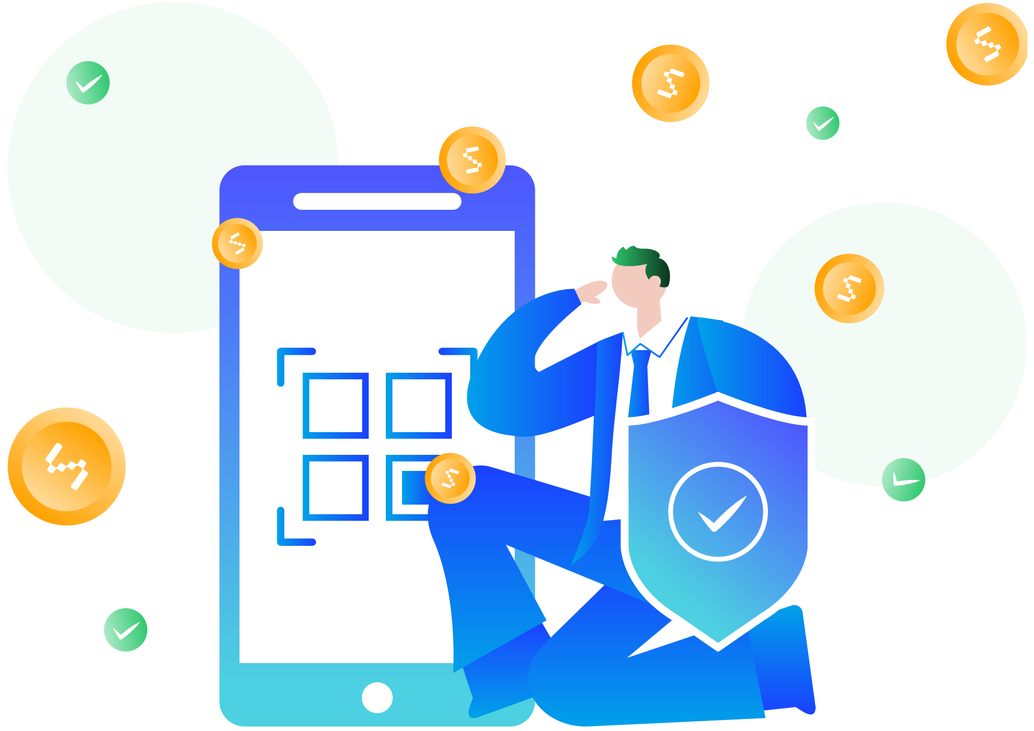
i. 以加密方式（HTTPS）傳輸敏感性資料。
ii. 通訊時應採用憑證驗證機制，以確保通訊對象的正確性，降低遭受中間人攻擊風險。
iii. 避免使用過舊的 TLS 版本，演算法也應採用 AES、3DES 演算法，以及 2,048 位元以上的 RSA，或是 224 位元以上的 ECC 加密演算法。

行動設備端 / 使用者端

i. 系統應即時 / 定期進行安全性更新。
ii. 商家應避免使用靜態的 QR Code，採用 QR Code 的驗證機制 (QR Code 共用平台)、規範行動支付軟體與系統之安全檢測及加強資安防護通報。
iii. 避免將密碼或加密金鑰等機敏資訊硬編輯至程式碼中。
iv. 採用反逆向工程的開發措施。
v. 盡可能驗證運行程式碼的完整性，確保未被植入後門。
vi. 遵守行動支付軟體與系統之安全檢測，包含弱點掃描、滲透測試、程式原始碼掃描與黑箱測試。
vii. 落實 PCI-DSS 驗證稽核。
viii. 應用程式運行應確認行動設備未被破解。
ix. 應用程式應避免含有常見的行動設備安全風險，如 OWASP Mobile Top 10 所述。
x. 加強員工資安意識及資安通報處理能力。
xi. 強化系統紀錄留存與證據保護機制。
xii. 採用適當的風險管理規劃。

國內行動支付相關規章

金融監督管理委員會於 2017 年修正了「電子支付機構資訊系統標準及安全控管作業基準辦法」，而中華民國銀行商業同業公會全國聯合會，亦修正「信用卡業務機構辦理手機信用卡業務安全控管作業基準」等法規，旨為建立相關電子支付安全控制基準，規範支付平台應具備完善之安全防護機制及維護使用者個資安全。此外數位發展部已修訂「行動應用 APP 基本資安規範」、「行動應用 APP 安全開發指引」，為針對行動應用程式之功能分類與安全要求範圍。至於保護卡片持卡人相關資料安全，支付卡產業安全標準協會 (Payment Card Industry Security Standards Council, PCI SSC) 制定一系列的安全標準 (PCI DSS)，除了規範儲存、處理或傳送持卡人資料外，也與資料處理過程所使用的設備或應用程式的開發有關，提供行動支付商家在開發及檢測 APP 時作為參考依據。



結論與建議

對企業與使用者而言，行動支付都是一種高成本效益且極為便利的支付服務。不論行動支付產業如何發展或變化，提供既便利又安全的交易環境永遠是企業的首要目標。針對行動支付產業未來可能面臨的各種挑戰，企業必須在便利與安全之間權衡取捨，不論抉擇為何，務須建立完善的風險管理機制，持續強化交易環境之安全防護，不僅是贏取使用者信任與忠誠的最大利器，也是勝出行動支付市場的成功關鍵。

CHAPTER 3

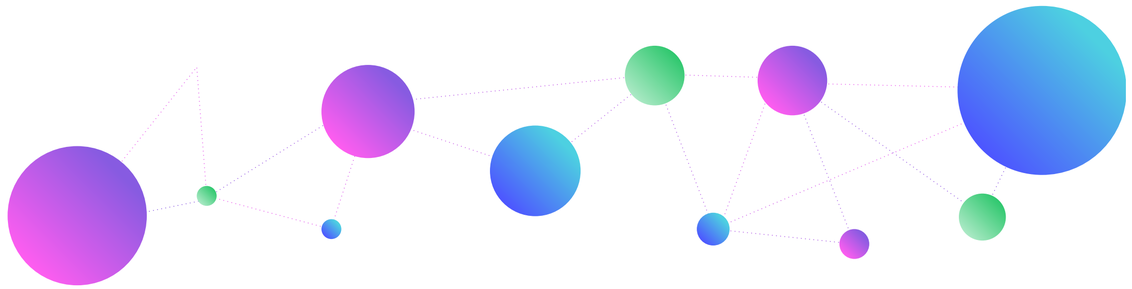
情資分享與漏洞協處概況

3.1 TWCERT/CC 資安情資分享

圖 22：TWCER/CC 資安跨域聯防與情資分享

在 2022 年 1 月至 12 月期間，TWCERT/CC 總計分享逾 110 萬筆之資安情資予相關單位 (因 2022 年新增處理情資類別：大量 TCP Middlebox reflection DDoS attacks 類情資，故情資數量較 2021 年高)，包含來自國際，欲針對國內 IP 位址進行協助與警示的通報；以及來自國內，欲針對國內其他單位或國際 IP 位址進行協處與警示的通報。情資來源主要為國際資安交流組織、國內資安相關組織、國內企業組織，以及各國電腦緊急應變小組 (Computer Emergency Response Team, CERT) 組織等相互交流的訊息。

收到資安通報後，TWCERT/CC 會依據通報中心之對象進行情資分享。依國內外對象區分，國內分享對象主要包含政府單位、網路業者、金融單位、學術單位、台灣駭客協會 HITCON 等資安組織，以及諸多國內企業；國外分享對象為 150 餘國家的 CERT/CSIRT 單位及相關資安組織。此外，為提升情資警示及分享效率，TWCERT/CC 通報系統與國家資安資訊分享與分析中心 (National Information Sharing and Analysis Center, N-ISAC)、美國自動化資安威脅情資共享計畫 (Automated Indicator Sharing, AIS)、反釣魚工作小組 (Anti-Phishing Working Group, APWG) 、英國 Netcraft、Phish Tank、TEAM CYMRU、Shadow Server 等國內外資安組織介接，定期並即時地進行情資分享互通交流，提升情資分享效能與聯防能量。



在 TWCERT/CC 所接獲並進行通報的情資中，以接受國際情資後分享至國內相關單位之數量為最大宗。而接收國內情資，將國內情資或資安訊息分享至國外的情資數量中，其通報的國家眾多，最多的為美國地區之國家，其次為中國、太平洋地區之國家，第三則為歐洲之國家，其詳細比例如圖 23：

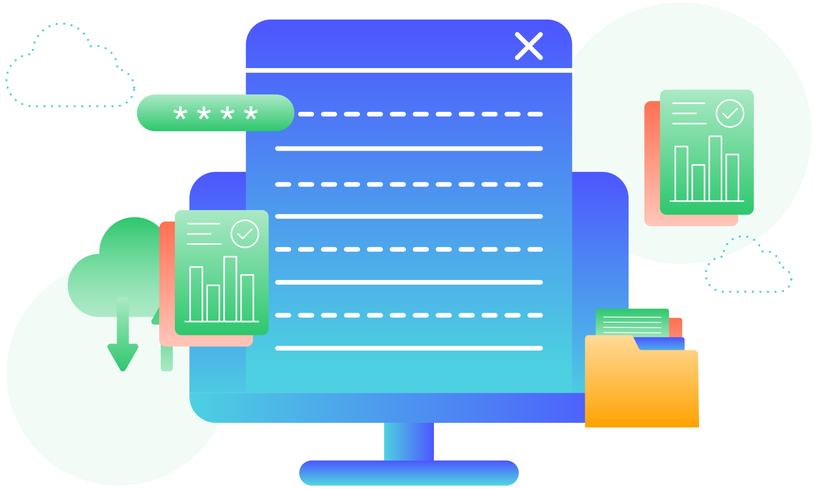
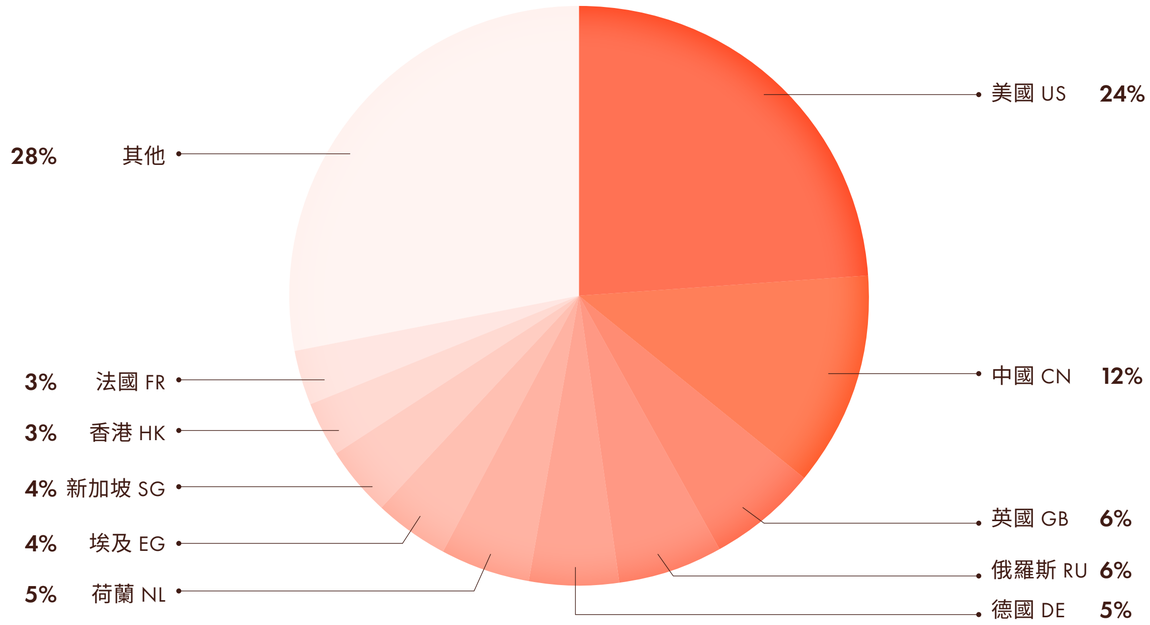


圖 23：TWCERT/CC 國際資安事件情資分享比例

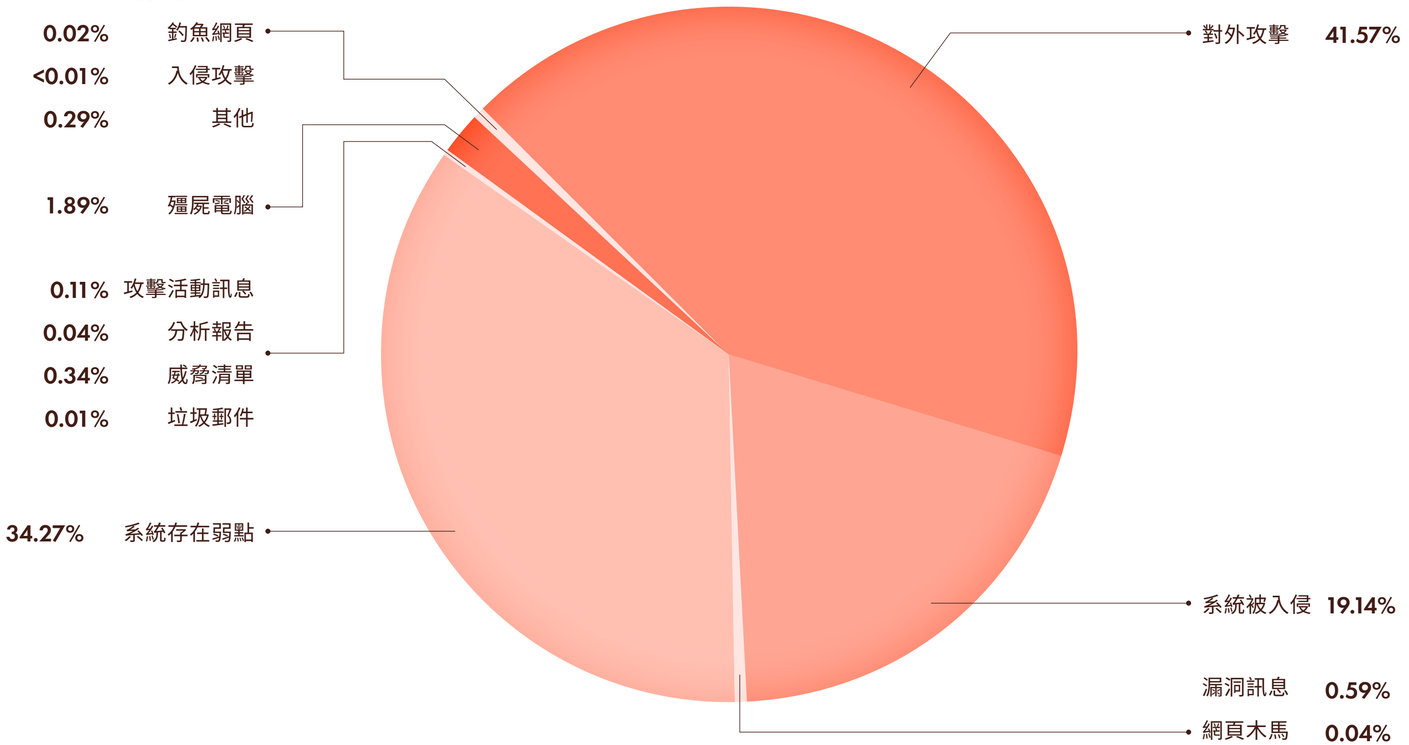


資料來源：TWCERT/CC 整理

TWCERT/CC 針對其攻擊類型及方式進行區分，接獲並通報國內組織的資安事件類型比例前三項分別為對外攻擊、系統存在弱點，與系統被入侵，代表有大量遭入侵的系統被利用作為攻擊用途。與 2021 年相比，系統被入侵有些微比例下降，但系統存在弱點佔比升高，即有被入侵風險，故亦需注意。

而對國內企業組織分享資安事件類型，前兩名為漏洞訊息與威脅清單，顯示 TCERT/CC 持續協助企業及時掌握最新資安訊息，強化防護能量與漏洞處理，以提升產品安全性；第三名則為系統疑存在弱點，代表仍有大量系統存有被入侵的風險，顯示企業組織對資訊安全意識仍需加強。

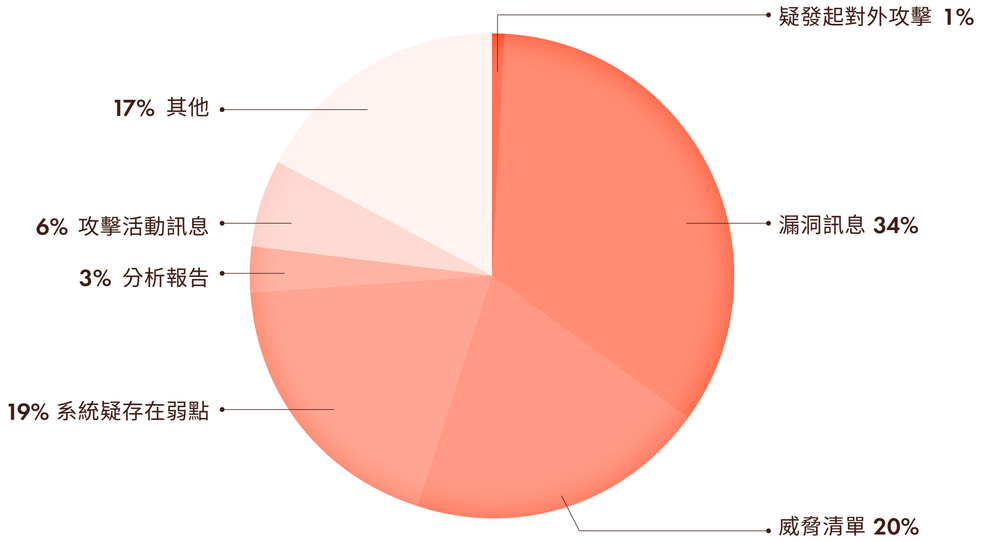
圖 24：TWCERT/CC 2022 境內情資分享威脅類型比例



資料來源：TWCERT/CC 整理

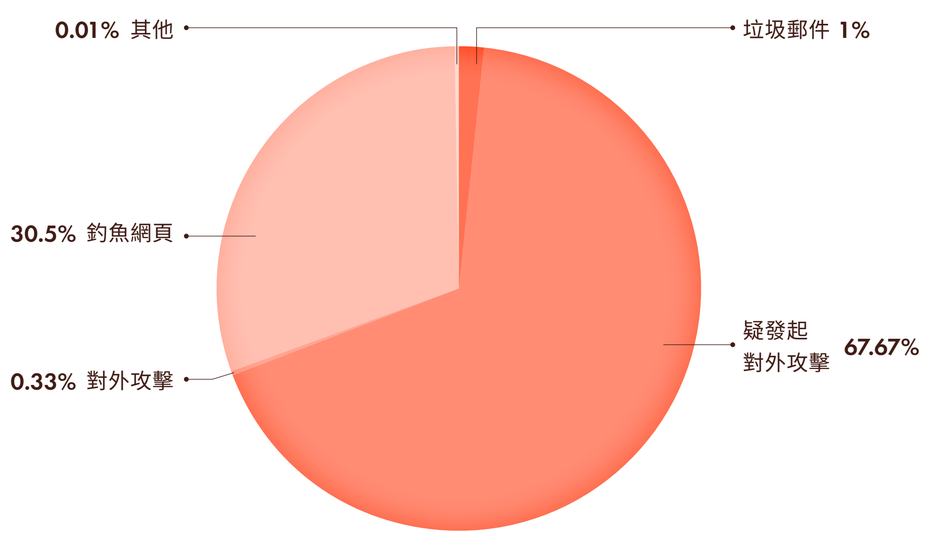
對國際單位分享的資安事件類型前三名為疑發起對外攻擊、釣魚網頁及垃圾郵件 (Spam)，主要為國際組織間之企業組織系統或主機因受攻擊者操控，導致其被利用對外發起惡意攻擊行為，或是對外寄送未經允許之垃圾郵件。與 2021 年相比，國外對外攻擊比例下降但國內比例上升，顯示國內組織受惡意程式攻擊日趨嚴重。

圖 25：TWCERT/CC 2022 對企業情資分享威脅類型比例



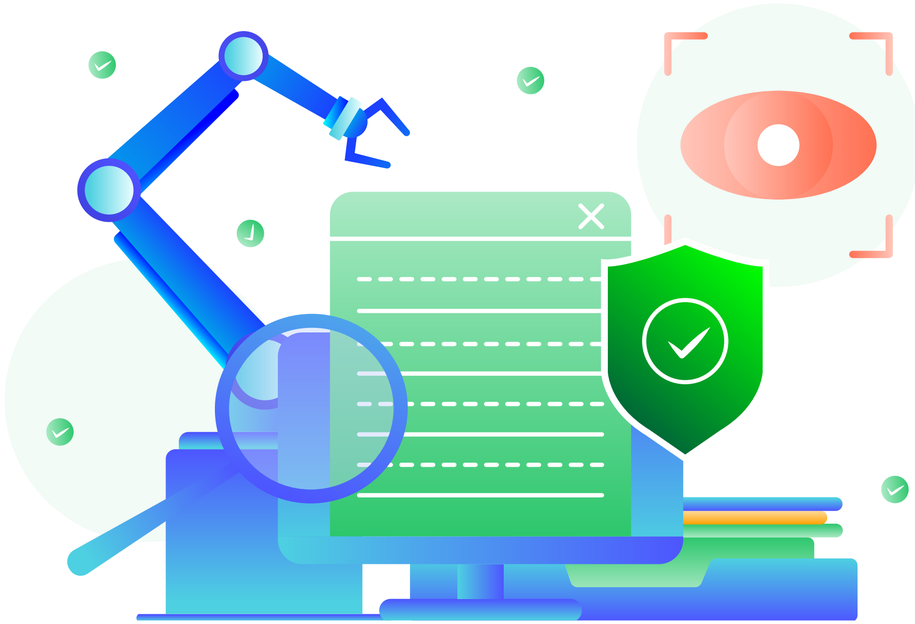
資料來源：TWCERT/CC 整理

圖 26：TWCERT/CC 2022 境外情資分享威脅類型比例



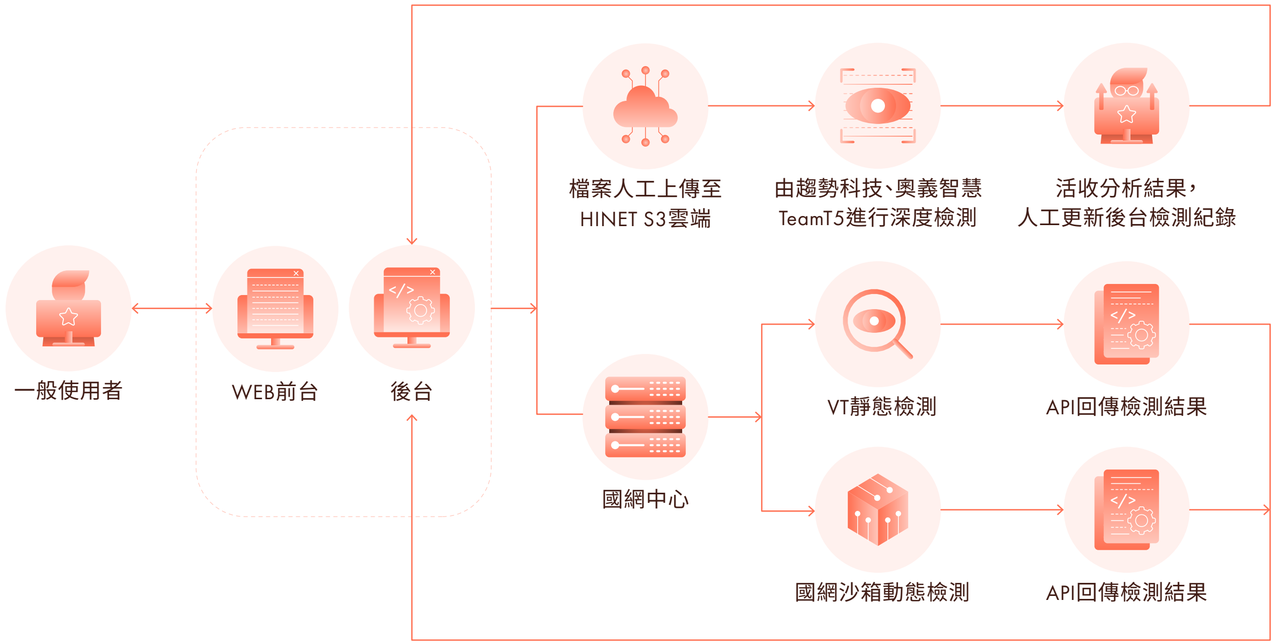
資料來源：TWCERT/CC 整理

3.2 VIRUS CHECK 惡意檔案分析



為協助企業與民眾降低被社交攻擊盜取機敏資料與入侵系統，TWCERT/CC建置惡意檔案檢測系統(Virus Check)，提供企業和民眾上傳可疑檔案以判別是否為惡意檔案。使用者上傳檔案後，Virus Check 透過靜態檢測與動態檢測，根據檔案行為或特徵判讀檔案風險類型(見表2)，以判別是否為惡意檔案，並與國網、趨勢科技、奧義智慧、TEAMT5等廠商合作，進行深度檢測提升準確度。

圖 27：Virus Check 惡意檔案檢測處理流程圖



資料來源：TWCERT/CC 整理

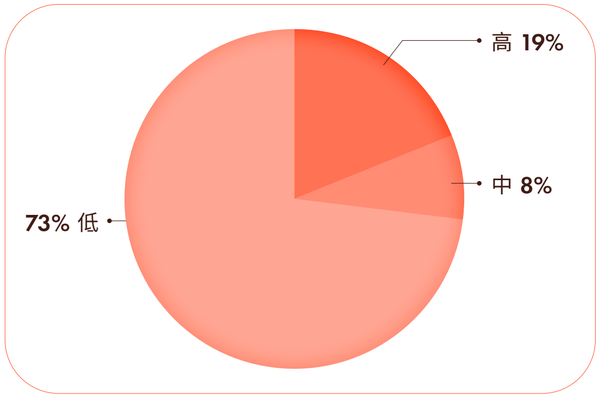
表 2: 惡意檔案風險類型

類型	判讀定義
低風險	檔案或程序具有大多良性程式會有的行為或特徵
中風險	檔案或程序具有良性應用程式也會有的可疑行為或特徵
高風險	檔案或程序具有惡意程式常有的可疑行為或特徵，例如執行上傳的 word 檔卻執行關閉防火牆功能。

資料來源 : TWCERT/CC 整理

2022 年 1 月至 12 月期間， TWCERT/CC 接獲二千多筆檔案，其中高風險檔案比例較 2021 年上升約 38%。

圖 28：TWCERT/CC 2022 Virus Check 檔案檢測風險值比例



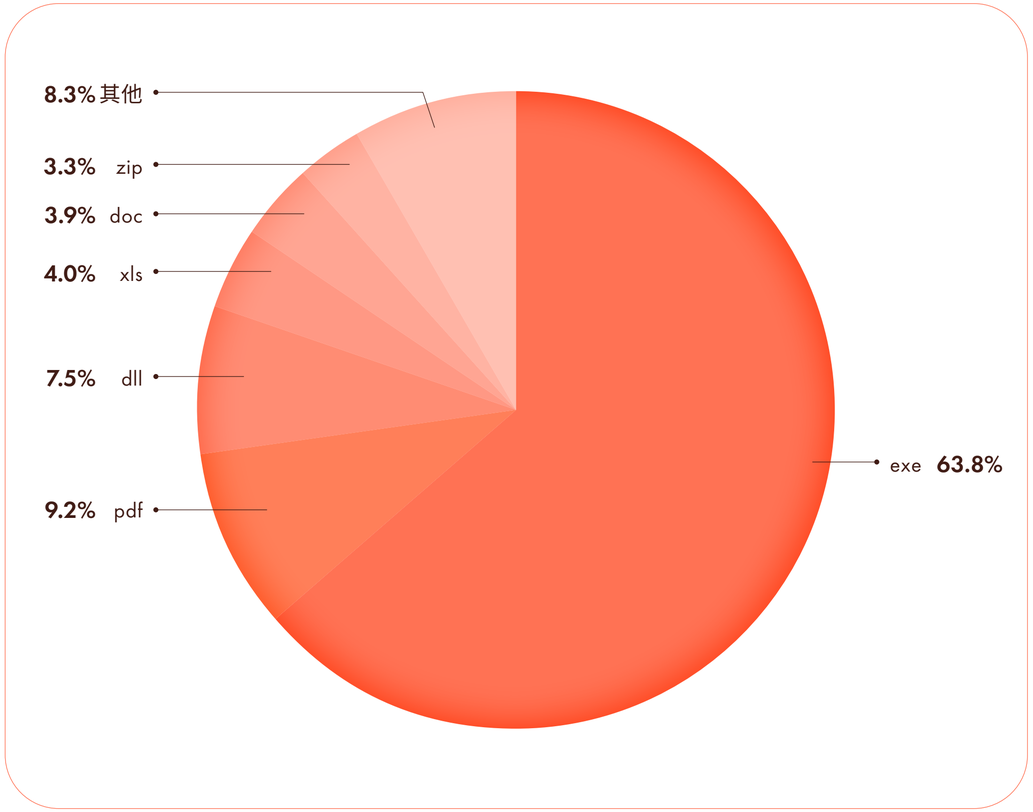
38%

高風險檔案比例較 2021 年上升

資料來源 : TWCERT/CC 整理

針對中高風險之檔案類型，2022 年 1 月至 12 月期間，共計逾 500 多個檔案中，數量最多前三名為可執行檔 exe 檔、可執行檔 pdf 檔與動態連結函式庫 dll 檔。與 2021 年相比，可執行檔 exe 檔佔比雖往下降但仍屬大宗。

圖 29：TWCERT/CC 2022 Virus Check 檢測檔案中高風險檔案類型比例



資料來源 : TWCERT/CC 整理

依據 111 年的情資，進而分析出我國 ICT 設備被利用對境外發起超過 52 萬餘次資安攻擊，簡略說明如下：

▣ IoT 類

- Conficker：利用 Windows 系統漏洞攻擊的威脅持續，擴大至大型 IoT 設備，如醫療的 MRI、CT 掃描器
- Sality(via P2P)：感染多廠牌的工控設備(IIoT)

▣ NAS 類

qsnatch 針對 NAS 設備感染，具持續改進感染方式

▣ 行動裝置類

android hummer 惡意軟體長期占據前四名

圖 30：111 年我國資通訊設備遭感染概況

▲ 上升 ▼ 下降 ◀▶ 持平 ✚ 新進

	2021/1	2022/2	2022/3	2022/4	2022/5	2022/6
1	android.hummer ▲	android.hummer ✚	conficker/downadup ▲	conficker/downadup ◀▶	sality ▲	sality ◀▶
2	conficker/downadup ▼	conficker/downadup ✚	android.hummer ▼	android.hummer ◀▶	conficker/downadup ▼	conficker/downadup ◀▶
3	virut ▲	virut ◀▶	qsnatch ✚	qsnatch ◀▶	qsnatch ◀▶	qsnatch ◀▶
4	lethic ▼	andromeda ▲	virut ▼	sality ▲	android.hummer ▼	android.hummer ◀▶
5	andromeda ◀▶	avalanche-generic ✚	andromeda ▼	virut ▼	virut ◀▶	virut ◀▶
6	coinminer ◀▶	android.bakdoor.prizmes ✚	android.bakdoor.prizmes ◀▶	andromeda ▼	andromeda ◀▶	andromeda ◀▶
7	android.bakdoor.prizmes ◀▶	coinminer ▼	coinminer ◀▶	coinminer ◀▶	avalanche-generic ▲	avalanche-generic ◀▶
8	avalanche-generic ◀▶	sality ▲	sality ◀▶	avalanche-generic ▲	likely-rat-netwire ✚	coinminer ▲
9	sality ◀▶	mozi ▲	avalanche-generic ▼	nymain ✚	coinminer ▼	m0yv ✚
10	mozi ◀▶	lethic ▼	mozi ▼	android.bakdoor.prizmes ▼	ranbyus ✚	likely-rat-netwire ▼
	2022/7	2022/8	2022/9	2022/10	2022/11	2022/12
1	sality ◀▶	conficker/downadup ▲	conficker/downadup ◀▶	conficker/downadup ◀▶	conficker/downadup ◀▶	conficker/downadup ◀▶
2	conficker/downadup ◀▶	qsnatch ▲	qsnatch ◀▶	qsnatch ◀▶	qsnatch ◀▶	qsnatch ◀▶
3	qsnatch ◀▶	android.hummer ▲	android.hummer ◀▶	android.hummer ◀▶	android.hummer ◀▶	android.hummer ◀▶
4	android.hummer ◀▶	sality ▼	sality ◀▶	m0yv ▲	sality ▲	m0yv ▲
5	andromeda ▲	m0yv ▲	m0yv ◀▶	sality ▼	m0yv ▼	sality ▼
6	coinminer ▲	likely-rat-netwire ▲	andromeda ▲	andromeda ◀▶	likely-rat-netwire ▲	likely-rat-netwire ◀▶
7	m0yv ▲	andromeda ▼	coinminer ✚	likely-rat-netwire ▲	avalanche-generic ✚	andromeda ▲
8	likely-rat-remcos ✚	likely-rat-remcos ◀▶	likely-rat-netwire ▼	coinminer ▼	likely-rat-remcos ▲	likely-rat-remcos ◀▶
9	likely-rat-netwire ▲	likely-rat-adwind ✚	avalanche-generic ✚	likely-rat-remcos ✚	andromeda ▼	likely-rat-orcus ✚
10	avalanche-generic ▼	likely-rat-im ✚	tinba ✚	likely-rat-adwind ✚	likely-rat-adwind ◀▶	likely-rat-firebird ✚

資料來源：TWCERT/CC 整理

3.3 資安漏洞協處

TWCERT/CC 參與美國非營利組織 MITRE 通用漏洞揭露計畫 (Common Vulnerability and Exposure, CVE)，擔任台灣區 CVE 編號管理者 (CVE Numbering Authority, CAN)，負責接收、審核及發布資安漏洞 CVE 編號，以降低資安漏洞對使用者及廠商所可能帶來的威脅，並透過台灣漏洞揭露平台 (Taiwan Vulnerability Note, TVN) 公布 CVE，供廠商、組織以及大眾查閱與引用。

1

我國發布之產品漏洞概況

在 2022 年期間，TWCERT/CC 總計接發布 101 個資安漏洞，其中有 79 個漏洞是軟體服務系統、有 22 個漏洞分屬於 IoT 設備，其中大多數漏洞通報來源為資安人員，先前 2021 年漏洞類型最多者為 Broken Access Control(權限控制失效)。而 2022 年漏洞類型最多者為 Path Traversal，顯示為開發過程中常忽略的權限控管不當的問題，導致攻擊者可存取到權限以外的目錄，TWCERT/CC 2022 審核發布 CVE 統計如下表 :

表 3： TWCERT/CC 2022 審核發布 CVE 統計表

類型	產品類別	數量	編號
軟體服務系統	牙醫管理系統	2	CVE-2022-22055、CVE-2022-22056
	安裝套件	1	CVE-2022-22262
	自然人憑證元件	1	CVE-2020-12775、CVE-2022-32959、CVE-2022-32960、CVE-2022-32961、CVE-2022-32962、CVE-2022-35222
	停車場管理系統	1	CVE-2022-25594

類型	產品類別	數量	編號
軟體服務系統	門禁考勤系統	1	CVE-2022-26671
	全方位系統	2	CVE-2022-26675、CVE-2022-26676
	IT 監控與管理軟體	2	CVE-2022-26668、CVE-2022-26669
	線上儲存服務	1	CVE-2022-26672
	企業流程管理系統	3	CVE-2022-32456、CVE-2022-32457、CVE-2022-32458
	企業溝通協作系統	3	CVE-2022-32958、CVE-2022-35220、CVE-2022-35221
	電子郵件行銷追蹤	1	CVE-2022-35223
	分析系統		
	健保卡網路服務元件	4	CVE-2021-45918、CVE-2022-35217、CVE-2022-35218、CVE-2022-35219
	行動入口網	1	CVE-2022-38118
	人資管理系統	1	CVE-2022-38116
	行銷發送系統	4	CVE-2022-32963、CVE-2022-32964、CVE-2022-32965、CVE-2022-35216
	整合系統控制軟體	1	CVE-2022-38699
	高階資訊戰情室	7	CVE-2022-39029、CVE-2022-39030、CVE-2022-39031、CVE-2022-39032、CVE-2022-39033、CVE-2022-39034、CVE-2022-39035
	校園網頁管理平台	1	CVE-2022-39053
	企業旅遊管理系統	1	CVE-2022-39054
	即時通訊軟體	1	CVE-2022-38117
	企業資訊入口管理平台	7	CVE-2022-39021、CVE-2022-39022、CVE-2022-39023、CVE-2022-39024、CVE-2022-39025、CVE-2022-39026、CVE-2022-39027

類型	產品類別	數量	編號
軟體服務系統	企業資訊入口管理平台	7	CVE-2022-39021、CVE-2022-39022、CVE-2022-39023、CVE-2022-39024、CVE-2022-39025、CVE-2022-39026、CVE-2022-39027
	全方位電子郵件管理專家	2	CVE-2022-40741、CVE-2022-40742
	監控軟體	4	CVE-2022-38119、CVE-2022-38120、CVE-2022-38121、CVE-2022-38122
	企業流程管理系統	3	CVE-2022-39036、CVE-2022-39037、CVE-2022-39038
	電子郵件系統	2	CVE-2022-41675、CVE-2022-41676
	人力資源發展系統	4	CVE-2022-39039、CVE-2022-39040、CVE-2022-39041、CVE-2022-39042
	跨平台數位簽章	3	CVE-2022-46304、CVE-2022-46305、CVE-2022-46306
	知識管理系統	1	CVE-2022-46309
	運維管理平台	1	CVE-2022-48229
	線上學習測驗平台	3	CVE-2022-43436、CVE-2022-43437、CVE-2022-43438
IoT 設備	路由器	13	CVE-2021-44158、CVE-2022-22054、CVE-2022-23970、CVE-2022-23971、CVE-2022-23972、CVE-2022-23973、CVE-2022-25595、CVE-2022-25596、CVE-2022-25597、CVE-2022-26670、CVE-2022-26673、CVE-2022-26674、CVE-2022-40740
	筆記型電腦	1	CVE-2022-21933
	USB 讀卡器驅動	1	CVE-2022-21742
	Bluetooth Mesh SDK	4	CVE-2022-25635、CVE-2022-26527、CVE-2022-26528、CVE-2022-26529
	電子配電器	2	CVE-2022-32966、CVE-2022-32967
	錄影主機	1	CVE-2022-47618

資料來源：TWCERT/CC 整理

國際資安事件與漏洞協處案例

▣ 微軟 Exchange Server 漏洞

TWCERT/CC 於 2022 年 2 月起持續接獲國際情資指出，來自俄羅斯的新殭屍網路惡意程式 Cyclops Blink，鎖定 WatchGuard 的防火牆設備，對此 WatchGuard 發布安全指引並建議所有用戶，不管有無受到 Cyclops Blink 感染，都應升級到最新的 Fireware OS，我國與該漏洞相關情資總計近 43 筆 IP 受駭，相關受害 IP 已全數通報完畢。又於 3 月接獲國內網通大廠通報，Cyclops Blink 新變種針對該網通大廠生產之路由器發動駭侵攻擊。TWCERT/CC 將相關情資與修補資訊，分享給聯盟成員和相關 ISAC 成員、通報國外 CERT 組織、同時亦發布相關新聞分享於官網、社群媒體等通知民眾和企業注意並更新，及早因應，降低駭侵事件擴散，以達聯防之目的。

▣ Cobalt Strike Beacon 惡意檔案情資分享

TWCERT/CC 於 2022 年 5 月接獲國際情資指出，名為 vmhost[.]exe 的惡意軟體檔案經分析後，確認為 Cobalt Strike Beacon loader/stager，Cobalt Strike 是被惡意攻擊者廣泛使用的攻擊工具，其中的 Beacon 是 Cobalt Strike 預設功能模組的名稱，功用是建立與 Command and Control (C2) 伺服器的連線，並在成功建立連線後下載完整的 beacon payload，做為後續攻擊的準備。TWCERT/CC 於次日將相關情資與修補資訊，分享給聯盟成員和相關 ISAC 成員，讓聯盟成員及早因應，降低駭侵事件擴散，以達聯防之目的。

▣ GootLoader 多階段攻擊情資分享

TWCERT/CC 於 2022 年 11 月接獲關於多階段的攻擊行為的情資，多階段攻擊是將攻擊分為多個不同階段，每個階段都執行一個攻擊行為的部分動作，而不是將整個攻擊行為一次完成，這可以讓攻擊行為更加隱蔽。此情資的惡意檔案為 GootLoader，後續可再下載 zip 壓縮檔，解開後則為 JavaScript 檔案，執行後會植入 Cobalt Strike Beacon 模組，並與 Cobalt Strike 伺服器建立連線，為之後繼續下載其它 Cobalt Strike 功能做好準備。經分析確認 Cobalt Strike 是被惡意攻擊者廣泛使用的攻擊工具，能提早偵測或阻斷 Beacon 的動作，就可以中斷攻擊的進程。TWCERT/CC 於次日將此情資訊分享給 CERT/CSIRT 聯盟成員和相關 ISAC 成員 (T-ISAC、E-ISAC、N-ISAC)。

▣ 國際資安情資分享通報

TWCERT/CC 多次接獲國際資安組織通知我國具有資安漏洞的資訊系統情資。TWCERT/CC 為避免漏洞遭駭客利用，造成國內相關單位或企業受駭侵，隨即進行情資彙整與分析；並將此漏洞資訊分享給 CERT/CSIRT 聯盟成員和相關 ISAC 成員 (T-ISAC、E-ISAC、N-ISAC 等)，及相關企業組織，以達重要資安情資分享，資安聯防之目的。

表 4：國際資安情資分享

月份	情資說明	筆數
110/6	Sonic Wall unpatched and end-of-life (EOL) 8.x firmware	62
110/8	Exchange Server	633
110/9	Fortinet VPN credential leaks	719
110/11	SQL Injection	195

資料來源 : TWCERT/CC 整理

3

國內資安事件與漏洞協處案例

▣ Deadbolt 勒索軟體

TWCERT/CC 自 2022 年 1 月以來陸續接獲通報，Q 牌與 A 牌 NAS 設備遭勒索軟體入侵，TWCERT/CC 經分析資料，確認為 Deadbolt 勒索軟體繼 Q 牌 NAS 設備後，新增 A 牌 NAS 為攻擊對象。TWCERT/CC 與 A 牌廠商合作，提供 TWCERT/CC 所接獲之資訊及建議緩解措施，如：(1) 關閉 Port Forwarding，(2) 關閉 NAS 系統管理的 Port 8080、443，(3) 更改 NAS 遠端 Web 存取預設 port 等。並將相關情資與修補資訊，分享給聯盟成員和相關 ISAC 成員、通報國外 CERT 組織、分享於官網、社群媒體等，提醒相關使用者及早因應，降低駭侵事件擴散，以達聯防之目的。

▣ 某製造大廠遭勒索攻擊情資分享

2022 年 1 月中旬我國知名製造大廠遭受 Conti 勒索軟體攻擊，TWCERT/CC 深怕此攻擊亦會針對國內相關或其他企業發動，便積極透過聯盟會員機制與該製造大廠聯繫，除了協助其應處，並獲得相關資訊分享給其他企業。經獲得受駭企業授權，去識別化後分享此次資安事件相關威脅指標包含中繼站資訊、病毒資訊、駭客入侵威脅指標 (Indicator of Compromise，IoC)、駭客入侵攻擊策略 (Tactics, Techniques, and Procedures，TTPs)、主機重建確認事項等情資與建議，分享給聯盟及 ISAC 相關成員，以利進行相關防護與自我檢測。

圖 28：TWCERT/CC 2022 Virus Check 檔案檢測風險值比例

Common attack techniques

釣魚信件裝後門
- 透過不安全釣魚信件進行安裝後門

獲得初始訪問權限
- 帳號被盜用
- 透過 Trickbot, BazarBackdoor 訪問系統

弱點遭利用
- 對外開放存取城市存在漏洞，可以被加以利用
- 例如 : 利用 Log4j 的 Powershell, Proxyshell 等已知漏洞進行攻擊

橫向擴大攻擊範圍
- 對網路進行滲透掃描
- 使用 Cobalt Strike 和 C2 server 進行連線控制
- 尋找安全層級較弱的主機進行攻擊

勒索軟體執行加密
- 透過 AnyDesk 等工具將機敏資料傳送到外部
- 機敏檔案被加密

Defenese

資安意識
- ✓ 提高資安意識，不隨意開啟可以連結、來源不明電子郵件、檔案

存取控制
- ✓ 針對外部來源的使用者，使用多重身分驗證
- ✓ 實施網絡分段和過濾流量，減少勒索軟體散播的可能

系統更新
- ✓ 使用專業的防毒軟體並確保安全控管正常開啟與運行，定即時進行更新
- ✓ 定期對軟體和應用程式進行漏洞評估，並進行補修和更新

網路監控
- ✓ 調查任何味精受玄的應用程式，尤其是遠端桌面或遠程監控的管理程式

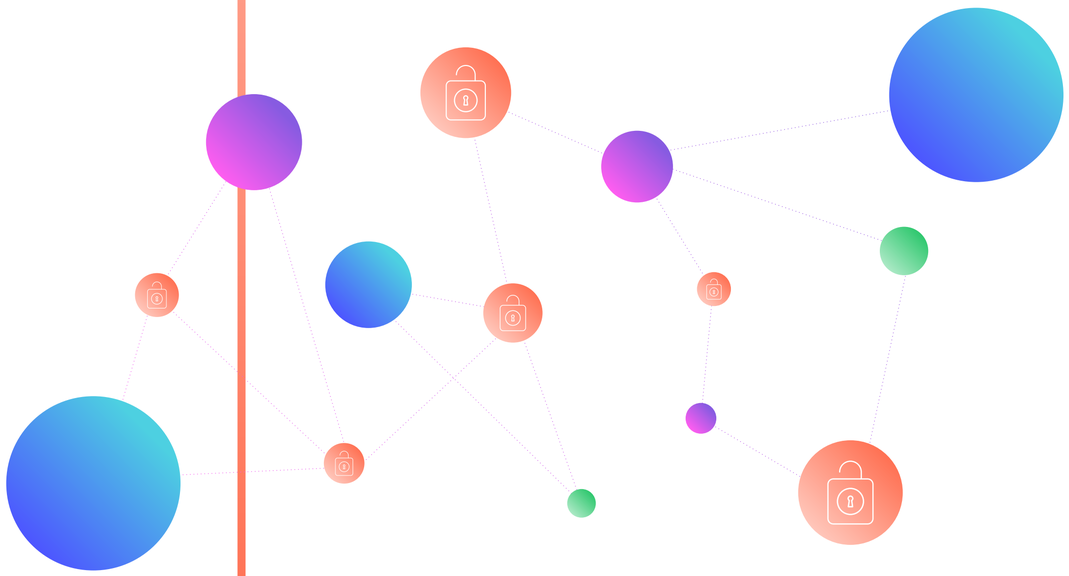
資料保全
- ✓ 定期進行檔案備份，並遵守 321 原則 :
  1. 資料至少備份 3 分
  2. 使用 2 種以上不同的備份媒介
  3. 其中 1 份備份要存放異地

資料來源 : TWCERT/CC 整理

▣ 某科技大廠通報疑似遭惡意程式入侵

2022 年 3 月接獲某科技大廠通報疑似遭惡意程式入侵 (偽裝為防毒軟體安裝檔，誘騙執行)，經檢測分析產製相關 IoCs 並提供防護建議，讓企業及早偵測阻絕。

經 TWCERT/CC 團隊研析此惡意程式為 Fsysna Trojan 惡意檔案，此惡意檔案兼具挖礦與勒索行為，潛伏時挖礦，擴散、蒐集資料後可轉而進行勒索攻擊。具強大橫向擴散能力，以 Mimikatz 搜集使用者憑證，並透過 SMB 服務嘗試感染。



▣ 某塑膠大廠駭侵相關情資分享及協助其確認修補情形

2022 年 5 月國內高科技公司通報 TWCERT/CC，該公司遭到外部 Emotet 信件攻擊，經分析其攻擊源來自 80 域名共 100 個信箱，透過發送信件給該公司內部 500 餘位員工。信件主旨以：Re/Fwd(員工名) 之標題信件，及變造發送端顯示名稱為該公司內部同仁，以降低員工的戒心。

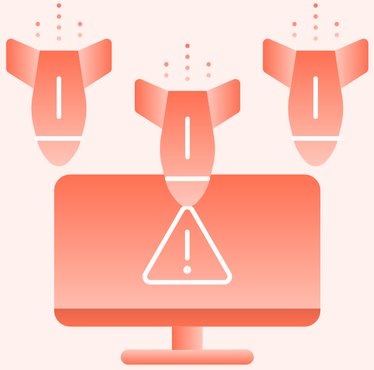
若有員工啟動巨集後，將會連至惡意程式載點，下載惡意程式，並註冊入系統服務，此時將會開始持續連線至中繼站接收指令，駭客得以利用受害設備發動攻擊。經該企業授權分享此次資安事件相關威脅指標等資訊，TWCERT/CC 彙整相關資訊，入侵威脅指標 (Indicator of Compromise，IoC)、駭客入侵攻擊策略 (Tactics, Techniques, and Procedures，TTPs)，提供分享給聯盟及 ISAC 相關成員，以利進行相關防護。

圖 32：分享給聯盟成員、相關 ISAC 成員以利進行相關防護

資安訊息 -ANA 攻擊活動訊息

防護建議

- 不要打開可疑的電子郵件附件或點擊電子郵件內文中的可疑連結
- 確保員工經過充分資安培，具備可疑的電子郵件連結和附件的能力
- 作業系統、應用程式和安全軟體應保持最新狀態
- 採用郵件防護系統，偵測與過濾垃圾郵件
- 採用應用程式管控，預設阻擋 PowerShell
- Emocheck 偵測工具
  https://github.com/JPCERTCC/EmoCheck/relrases/tag/v2.3.1



資料來源 : TWCERT/CC 整理

CHAPTER

合作交流與資安推廣

4.1 主辦活動

為掌握資安趨勢，TWCERT/CC 積極參與國內外重要資安會議及實務交流等活動，建立溝通管道，強化資安協處效率。並且為提升大眾之資安意識與資安事件通報意願，TWCERT/CC 更積極主辦相關資安通報應變研討會，強化資安聯防能量。

1

台灣資安通報應變年會

2022 年台灣資安通報應變年會活動，除了以往的宣導資安通報意識與資安通報意願外，更以強化台灣公私部門「超前佈署，資安聯防」的概念與執行作法，進行資安應變防護、企業建置資安相關政策或組織、國內 ISAC 組織之經驗分享。

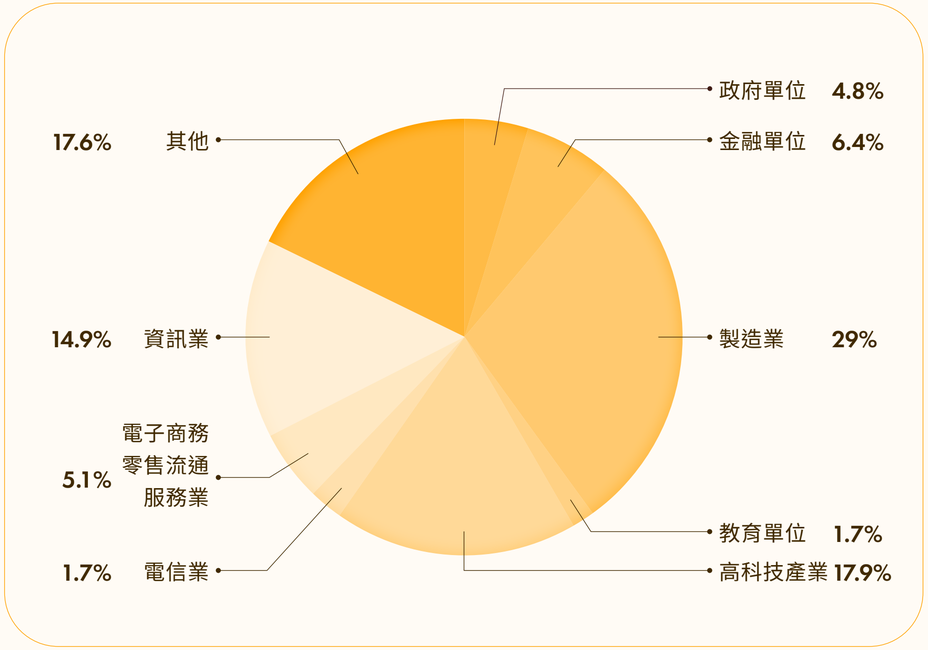
本次活動以「資安韌性，營運永續」為核心主題，邀請國家通訊傳播委員會孫雅麗委員，說明了 5G 萬物聯網時代的安全供應鏈管理與 NCC 的 3 個創新作為。同時，面對全球共通的勒索攻擊威脅，規劃了國際資安趨勢座談，由台灣網路資訊中心黃勝雄執行長主持，邀請美國國土安全部網路安全暨基礎設施安全局（CISA）科長（Section Chief）Patricia A. Soler、微軟威脅情資中心（MSTIC）Benjamin Koehl、卡內基美隆大學軟體工程學院電腦緊急應變團隊代表 Christopher Rodman，與馬來西亞 MyCERT 專家 Sharifah Roziah Mohd Kassim，探究網路資安風險與解決方案。現場還邀請了奧義智慧共同創辦人邱銘彰、法務部調查局資安工作站主任鄭健行等專家進行議題分享。

國立陽明交通大學資訊工程學系教授林盈達，主持產業資安高峰座談會，與高科技資安聯盟召集人暨合勤投控資安長游政卿、資安長聯誼會會長暨鴻海研究院執行長李維斌、台灣資安主管聯盟副會長暨台達電子資訊長曾立峰等大廠專家，以企業角度分享如何面對資安威脅。

圖 33：台灣資安通報應變年會活動剪影

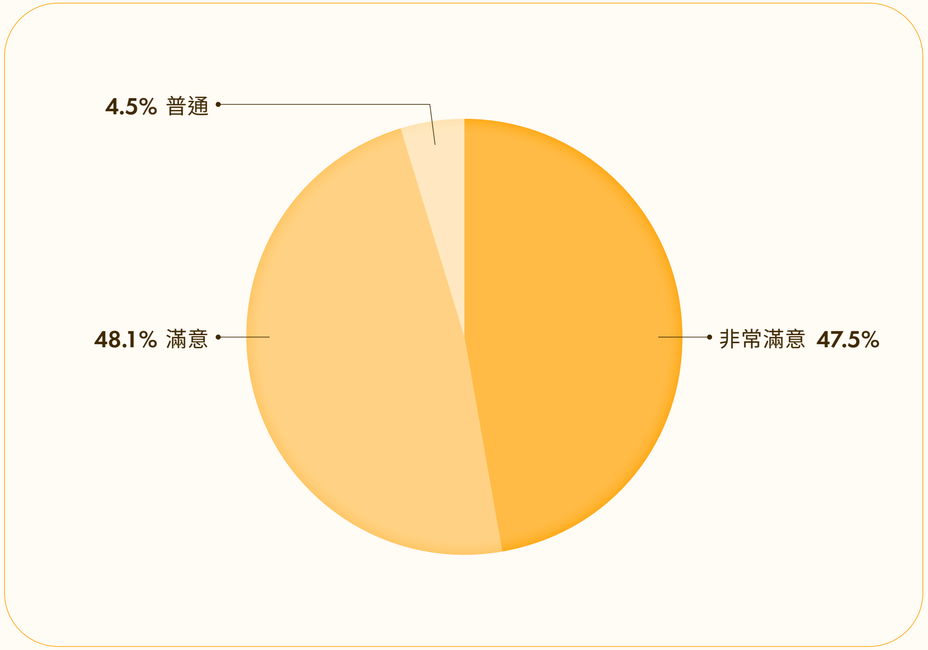
本次活動與會之線上與現場人數總計 940 人，與會者對兩場專題座談與專題演講都非常有興趣，更認為本次應變年會對企業及未來資安政策制定意義相當重大，超過 95% 的與會者期待明年再次參加資安應變研討會。與會人員以製造業為大宗，占總人數 29%，依序為高科技業與資訊業。

圖 34：聽眾出席行業別分析



資料來源：TWCERT/CC 整理

圖 35：研討會整體滿意度圖



資料來源：TWCERT/CC 整理

從整體統計分析顯示，此次台灣資安通報年會已確實達到宣傳資安意識、提升品牌認知、增添資安通報意願與強化台灣公私部門「超前佈署，資安聯防」的概念與執行作法之目的。

台灣 CERT/CSIRT 聯盟交流會議

加強民間資安情資分享與資安聯防，TWCERT/CC 鏈結資安單位與企業能量，組成之「台灣資安聯盟」，以多元情資分享管道，達到跨域資安威脅聯防之綜效。

成員可透過聯盟彼此交換資安情資，針對營運面遭遇資安問題或近期發現之重要資安議題進行探討與分享，以達資安聯防之目的，並增進台灣整體資安防護能力。

2022 年度除了召開聯盟成員會議，分享資安新資訊和聯盟成員進行資安資訊交流外，亦舉辦三場教育訓練，協助聯盟成員提升資安能力，強化台灣資訊安全的防護網。

▣ 聯盟成員會議

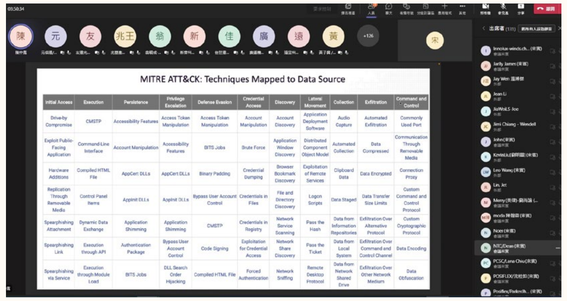
共有 66 個單位 77 位成員參與。本次會議邀請奧義智慧科技創辦人邱銘彰，分享「AD 入侵路徑可視化」，做為會員強化 AD 安全性的參考。BV 資訊安全部 / 首席資安專家林上智及聯盟成員網擎資訊劉中仁研發協理，以透過真實的郵件伺服器駭侵事件，分享各種資安威脅攻擊樣態。統計本次聯盟會議的會後滿意度調查，參與學員的整體滿意度為 4.67；而對於本次會議邀請講者分享內容滿意度為 4.68 (本滿意度調查採 5 分法尺度)。

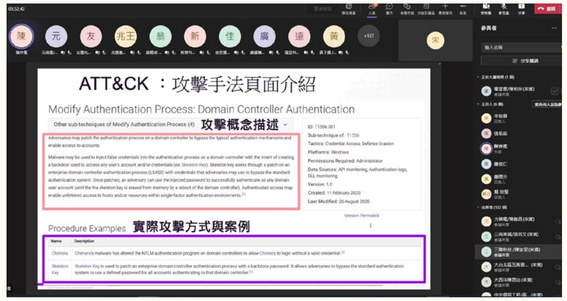
圖 36：2022 年「台灣 CERT/CSIRT 聯盟」聯盟會議合影

▣ 「台灣 CERT/CSIRT 聯盟」資安教育訓練 (一)

本次教育訓練以線上及實體混合方式辦理，講師以威脅獵捕為題，帶領聯盟成員進行實機操作，體驗如何在企業內部找出可能的駭客攻擊軌跡。本次活動共計 142 個單位 179 位 (實體 :31 、線上 :148) 與會者參加，針對本次教育訓練，參與學員的整體滿意度 4.67 (本滿意度調查採 5 分法尺度)。

圖 37：2022 第一次「台灣 CERT/CSIRT 聯盟」資安教育訓練實況





▣ 「台灣 CERT/CSIRT 聯盟」資安教育訓練 (二)

本次教育訓練以企業 Blue Team 資安演練為課程主軸，共辦理兩場，學員藉由 SIEM(Security Information and Event Management) 平台實機模擬真實 APT (Advanced Persistent Threat) 攻擊情境，發覺攻擊行為並分配資源進行事件調查，同時學員也能藉由本次教育訓練檢視自己的資安技能與加強資安應變能力。本次活動共計 52 個單位 83 位與會者參加，針對本次教育訓練，參與學員的整體滿意度 4.03。

圖 38：2022 年度第二次「台灣 CERT/CSIRT 聯盟」資安教育訓練實況

4.2 國際國內交流

2022 年 TWCERT/CC 參與多場國際交流會議，以了解國際資安發展之趨勢及現況，藉此提升 TWCERT/CC 自身的資安能量，從資安通報之分析、處理到資安意識推廣，擴及至國際間資安聯防。除參與國際會議外，並參加 2022 APDrill 國際網路安全攻防演練，以下為詳細介紹：

APEC TELWG 線上大會

亞太經濟合作會議 (APEC) 之電信暨資訊工作小組 (TELWG) 會議，為亞太 21 個經濟體之通訊領域發展現況報告之會議。本次會議 TWCERT/CC 與國家通訊傳播委員會、交通部郵電司、行政院國家資通安全會報技術服務中心、財團法人電信技術中心、財團法人全國認證基金會等單位共同參與。本次 APECTEL64 線上會議，TWCERT 負責參與亞太經濟體報告並進行內容摘要。另於 APEC Security and Prosperity Steering Group (SPSG) 會議提供 TWCERT 的「國情報告」及「SPSG 簡報」，說明在資訊安全議題上，台灣在跨國領域的資安聯防中所擔任的重要角色。

1

34TH Annual FIRST Conference

The Forum of Incident Response and Security Teams (FIRST) 為國際非營利組織，致力於促進全球各資訊安全應變小組及各領域資安人員間之合作與技術交流。探討議題包括資安政策、技術工具、通報應變流程處理等。本次參與會議主要目的在於了解 FIRST 國際組織之資安趨勢與現況，包含近年資安威脅、勒索軟體及產業鏈攻擊的趨勢，俄烏戰爭大規模網路攻擊技術分析、資安防護機制研析、國際間對 CSIRT 運行機制探討、通報應變及威脅情資平台分享相關之技術等，以提升國際聯防與 TWCERT/CC 資安通報之分析與處理能量。

NatCSIRT 2022 年會

國家電腦安全與事件應變小組會議 (National Computer Security Incident Response Team, NatCSIRT) 成員為各國國家級 CERT/CSIRT 組織。主要為促進國際 CERT 組織之間的合作交流，並針對國家安全、經濟、關鍵基礎設施等資安議題進行分享，TWCERT/CC 由丁綺萍副執行長進行 CERT 業務分享，說明 TWCERT/CC 在公私聯防的角色與作法，並與同樣參加 NatCSIRT 的 Cybersecurity and Infrastructure Security Agency(以下簡稱 CISA) 人員交流，TWCERT/CC 獲邀加入聯合網路防禦協作組織 (JCDC, Joint Cyber Defense Collaborative)，以利後續合作。

APNIC 54 論壇

APNIC(Asia Pacific Network Information Centre) 為掌管亞太地區 IP 位址與 AS 號碼發放的機構，為能廣納會員對於 IP 位址及 AS 號碼相關政策之意見，並進行網路管理相關技術交流，APNIC 每半年召開會議，以供各界對於其 IP 位址及 AS 號碼資源之政策作一個公開的討論。藉由對 IP 位址及 AS 號碼資源管理政策提案之公開討論的方式，依照與會會員所達成的共識，制訂成相關政策。TWCERT/CC 並於 APNIC FIRST Security 介紹近期台灣 Middlebox 漏洞概況，分享協處經驗 (An Anatomy of TCP Middlebox Reflection Attack and Mitigation Measures)。

APCERT Annual General Meeting (AGM)、APCERT Closed Conference、FIRST-APCERT Regional Symposium

APCERT Annual General Meeting (AGM) 為各 WG(Working Group) 現況報告之會議，APCERT Closed Conference 為主題演講會議，TWCERT/CC 與會分享包含 CERT NZ 對於線上網路安全行為研究、CyberSecurity Malaysia 對於各 CSIRTs 資安事件回覆處理機制，以及 CERT-PH 對於數位轉型之資安風險研究等內容。並參與為亞太地區舉辦的線上主題演講會議 (2022 FIRST Virtual Symposium: Asia Pacific Regions)。

APEC TEL

APEC TELECOMMUNICATION AND INFORMATION WORKING GROUP (APEC TEL WG) 旨在促進亞太地區的經濟體，於資通訊技術服務、資訊分享、政策規範之合作與成長，並致力於推廣各經濟體的資通訊安全。本次會議 (APEC TEL 65) 主要為亞太地區各經濟體之資安發展趨勢與現況報告，包括如資安意識推廣、數據隱私、勒索軟體、漏洞議題等，本次 TWCERT/CC 參與會議除了提供 SPSG 之國情摘要，並於會議中負責 APEC TEL 大會第 1、2 日及 SPSG 會議的報告摘要。藉參加此會議提升國際聯防，資安通報之處理能量。

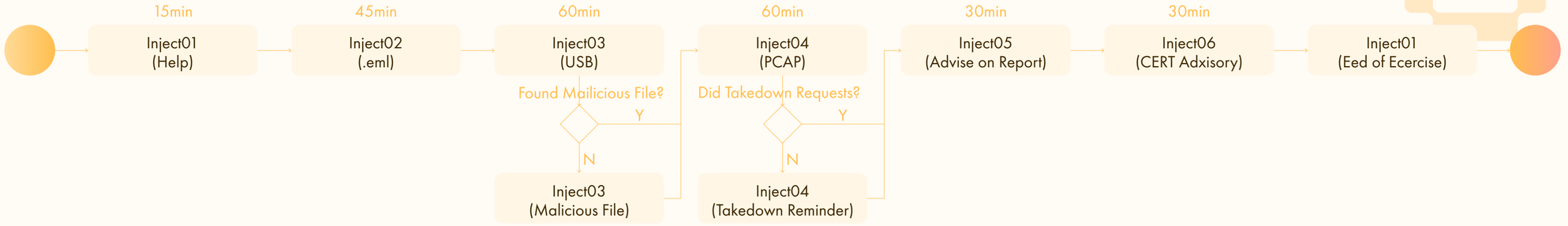
SANS APEC ICS Summit

為掌握國際工業控制系統 (Industrial Control Systems, ICS) 資安威脅與防禦的發展趨勢，TWCERT 參與由國際知名資安機構 SANS 舉辦的亞太區之工控安全研討會，由國際知名的工業控制系統安全專家，分別從管理面與技術面研討相關威脅趨勢與因應手段，進而掌握工控系統安全的防禦機制。強調應重視工業控制系統相關的資安偵測、防禦、事件應處 (incident response)，及供應鏈安全等機制。

參與國際網路安全攻防演練 – 2022 APDrill

本年度 Drill 活動由 Sri Lanka CERT/CC 主導策劃，演練主題討論會議 (Drill-WG) 討論訂出今年度演練主題為「Data Breach Through Security Malpractice」，並決議出演練中所需要進行分析情資的項目，包含 USB 映像檔分析、惡意腳本分析、惡意流量分析、釣魚郵件分析及相關情資整理及統整情資後的分享內容等。

圖 39：APDrill 2022 情境示意



資料來源：TWCERT/CC 整理

本次演練共有 32 個團隊參與，最終僅 2 個團隊能在無需解題提示，且於時間限制內完成所有的任務，TWCERT/CC 為其中之一。參與此次演練以累積 TWCERT/CC 成員的資安協處經驗，並將參與演練時所遇到的問題、想法，回饋至 TWCERT/CC 組織資安事件通報協處流程，進而提升整體協處流程的品質與效率。

4.3 資安推廣與分享

TWCERT/CC 企業資安推廣與分享

因資安議題相當廣泛，為了協助企業組織更精確地提升該產業之資安防護能量，TWCERT/CC 常與各產業協會合作交流，針對特定產業領域，進行演講或交流，藉此提升該產業成員及組織之資安意識與能量。

首先 TWCERT/CC 針對中小企業需求，分別與台中電腦公會及中山大學合作，於七個縣市舉辦「資訊安全防護及案例分享研討會」共計八場， 因應疫情以虛實混合方式辦理，總計逾五百人參與研討會，整體表現皆具高滿意度。

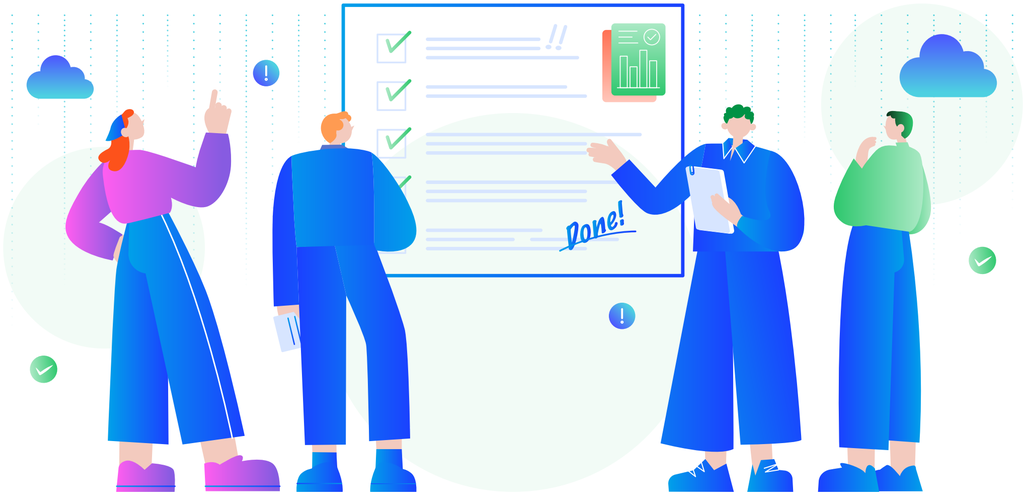


圖 40： 台中場「資訊安全防護及案例分享研討會」

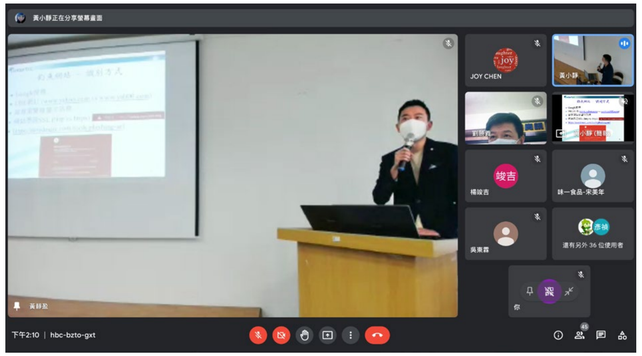
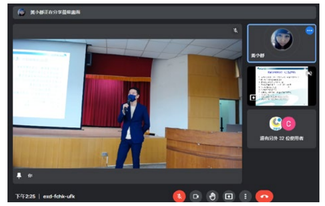


圖 41： 南投場「資訊安全防護及案例分享研討會」



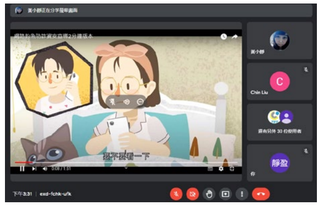


圖 42：桃園場「資訊安全防護及案例分享研討會」

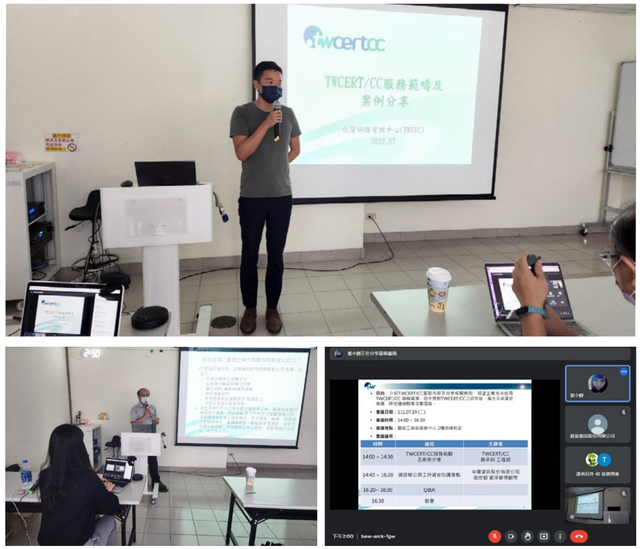


圖 43：高雄場「資訊安全防護及案例分享研討會」

圖 44：雲林場「資訊安全防護及案例分享研討會」

圖 45：嘉義場「資訊安全防護及案例分享研討會」

圖 46：台中場「資訊安全防護及案例分享研討會」

圖 47：台南場「資訊安全防護及案例分享研討會」

圖 48：「資訊安全防護及案例分享研討會」文宣

資料來源：TWCERT/CC 整理

TWCERT/CC 社群資安研討與分享

TWCERT/CC 除參與對企業推廣資安服務的活動外，亦以共同推廣單位參與多場國內交流會議，包含 ICANN APAC-TWNIC ENGAGEMENT FORUM(合作交流論壇)，及中華民國電腦稽核協會之會議。並且以共同舉辦或贊助方式參與特定社群的資安會議進行交流，例如第三十二屆全國資訊安全會議、HITCON PEACE 2022、CYBERSEC 2022 臺灣資安大會，及 2022 Cyberspace 聯合研討會，以下為詳細介紹：

3rd ICANN APAC-TWNIC ENGAGEMENT FORUM(合作交流論壇)

ICANN 及 TWNIC 舉辦合作交流論壇 (ICANN APAC-TWNIC Engagement Forum)，TWCERT/CC 為共同協辦。以合作交流論壇建立一個共同合作、討論與鏈結的全球網路社群，TWCERT/CC 藉此機會對國際相關組織推廣 TWCERT/CC 於國際資安情資分享之角色及任務。

TWCERT/CC 負責 Cyber Threat and Vulnerability Handling 議程，以座談會形式舉辦，邀請國立陽明交通大學林盈達講座教授主持，與談人有 APNIC、JPCERT/CC、Cyber Security Cloud 資安相關專家，針對資安事件處理、弱點通報等議題進行分享與探討。

圖 49：TWCERT/CC 協辦 ICANN APAC-TWNIC Engagement Forum

參與中華民國電腦稽核協會之「推動 ISACA ITAF 國際資訊稽核實務準則提升資訊風險、控制與安全之確保能力」會議

配合近年政府陸續發布「資通安全管理法」、「上市上櫃公司資通安全管控指引」等法規，如何落實資訊稽核程序也成為重要課題，國際電腦稽核協會 (ISACA) 最新發布之國際資訊稽核實務準則 (ITAF) 中文版，將可為國內從事內外部資訊稽核、顧問與諮詢服務人員，提供與國際有關稽核執行和有效稽核報告編制的同步指導。

本次活動 TWCERT/CC 向與會人士推廣說明，針對大多數的資安防禦，都會牽涉到跨域聯防，必須透過彼此之間的互助，方能達到最佳的防禦效果。而 TWCERT/CC 和國際上許多資安組織都有合作關係，因此，TWCERT/CC 可透過這些資安組織，掌握第一手的資通安全資訊，達到跨域聯防的重要效益。

圖 50：TWCERT/CC 參與中華民國電腦稽核協會之會議

第三十二屆全國資訊安全會議

由中華民國資訊安全學會舉辦的第三十二屆全國資訊安全會議，因 COVID-19 疫情影響改為全線上舉辦。TWCERT/CC 贊助並參與此會議，藉由此會議推廣 TWCERT/CC 資安通報服務，了解當前我國針對資訊安全相關的研究，及當前的資安領域研究方向。

HITCON PEACE 2022

與社團法人台灣駭客協會合作舉辦 HITCON PEACE 2022，於台北南港展覽館二館舉辦，此活動內容除了預測三至五年即將到來的資安趨勢，與提供目前可實踐應用的資安解決方案外，更加結合企業紅、藍攻防競賽展現真實力、並開放參與聽眾與海內外貴賓講師進行即時的網路交流互動。

圖 51：HITCON PEACE 2022

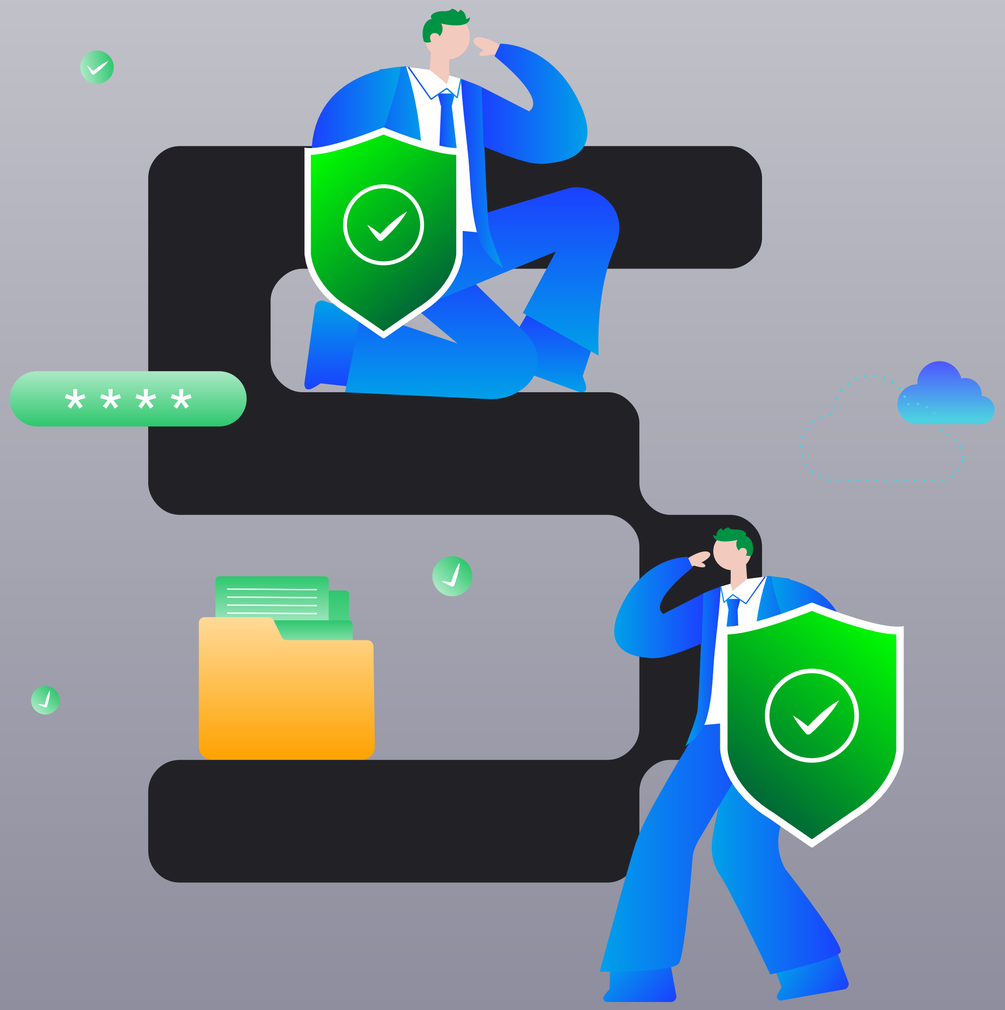
第 38 屆 TWNIC IP 政策資源管理會議

第 38 屆 TWNIC IP 政策資源管理會議，本次會議議題針對台灣及全球的新興網路服務的重要關鍵技術，及應用服務的發展趨勢進行研討交流。TWCERT/CC 的蕭信仁工程師介紹近期台灣 Middlebox 漏洞概況與 TWCERT/CC 的協處經驗分享 (An Anatomy of TCP Middlebox Reflection Attack and Mitigation Measures)。除此之外，TWCERT/CC 藉此推動資安事件情資分享以及應變通報之交流，強化國內資安防護能量。

圖 52：TWCERT/CC 參與第 38 屆 TWNIC IP 政策資源管理會議

第38屆TWNIC-IP政策資源管理會議 (上午場) 38th TWNIC IP Open Policy Meeting

CHAPTER



結語

5 結語

正如我們親身經歷過的一樣，2022 年全球仍受冠狀病毒疫情影響，企業組織與大眾多已習於遠距工作模式，以及各種雲端服務、社群媒體、行動支付及物聯網生活等。不論企業或個人皆蒙其利，享用著高度的效率與便利；然此同時，駭客組織及網路犯罪份子也致力於翻新攻擊戰術 / 技術，發展更多惡意軟體與變種病毒，駭客生態也朝雲端化、產業化演變，RaaS 勒索攻擊也可上網訂閱代操服務，Log4Shell 核彈級資安漏洞衝擊仍在，面對此新的趨勢，單打獨鬥資安防護已難對抗快速、複雜、有組織的持續性攻擊。

基於維護我國資通訊安全樞紐角色，TWCERT/CC 持續與國內外組織密切交流，擴大情資分享與聯防應變，才能與時俱進有效因應新挑戰。針對近期國際 STIX 標準更新，也將著手進行相關情資通報功能改版，以提升情資分享效率，達成強固整體網路安全目標。此外，亦積極主協辦及參與國內外組織交流合作，增加資安通報協處能量，結合公私部門資源，協助處理企業資安事件及提供事件處理參考指南，以增強企業組織資安應變能力，讓企業及民眾都有安全的網路環境可用。

參考書目

第二章 資安威脅與防護

[1].Akamai. TCP Middlebox Reflection: Coming to a DDoS Near You. https://www.akamai.com/blog/security/tcp-middlebox-reflection

[2].Kevin Bock, Abdulrahman Alaraj, Yair Fax, Kyle Hurley, Eric Wustrow, and Dave Levin. Weaponizing Middleboxes for TCP Reflected Amplification. In Proceedings of the 30th USENIX Security Symposium. https://www.usenix.org/system/files/sec21-bock.pdf

[3].Jack Edge. Weaponizing middleboxes. https://lwn.net/Articles/869842/

[4].Ravie Lakshmanan. Hackers Begin Weaponizing TCP Middlebox Reflection for Amplified DDoS Attacks. https://thehackernews.com/2022/03/hackers-begin-weaponizing-tcp-middlebox.html

[5].Shadowserver Foundation. Over 18.8 million IPs vulnerable to Middlebox TCP reflection DDoS attacks. https://www.shadowserver.org/news/over-18-8-million-ips-vulnerable-to-middlebox-tcp-reflection-ddos-attacks/

[6].Shadowserver Foundation. Vulnerable DDoS Middlebox Report. https://www.shadowserver.org/what-we-do/network-reporting/vulnerable-ddos-middlebox-report/

- Check Point Software Technologies Ltd. “Check Point Software's 2022 Security Report: Global Cyber Pandemic's Magnitude Revealed” https://pages.checkpoint.com/cyber-security-report-2022
- 趨勢科技 “2022 年資安年度預測報告” https://www.trendmicro.com/zh_tw/security-intelligence/threat-report.html
- NCCST “資訊安全議題案例分享” https://nicst.ey.gov.tw/File/D55C6E61DC0BE23?A=C
- “零信任網路專區” https://www.nics.nat.gov.tw/ZeroTrustMain.htm?lang=zh
- “Zero Trust Architecture ” https://csrc.nist.gov/publications/detail/sp/800-207/final
- Wikipedia. “Web3” https://en.wikipedia.org/wiki/Web3
- The Investopedia Team. “Web 3.0 Explained, Plus the History of Web 1.0 and 2.0” https://www.investopedia.com/Web-20-Web-30-5208698
- Wikipedia. “ Semantic Web” https://en.wikipedia.org/wiki/Semantic_Web
- ConsenSys. “An Introduction to IPFS” https://medium.com/@ConsenSys/an-introduction-to-ipfs-9bba4860abd0
- Cisco Talos. “The 5 most common security concerns in the emerging new Web 3.0 world”
- Linux hint. https://linuxhint.com/Web-3-security-implications/207/final
- Keith D. Foote. “A Brief History of Cloud Computing” , DATAVERSITY, Dec. 17, 2021 https://www.dataversity.net/brief-history-cloud-computing/ (瀏覽日期：2022 年 8 月 21 日)
- SP 800-145. “The NIST Definition of Cloud Computing” , NIST, Sep. 2011 https://csrc.nist.gov/publications/detail/sp/800-145/final (瀏覽日期：2022 年 8 月 22 日)
- Matt Mcdermott. “Cloud Computing: Benefits, Disadvantages & Types of Cloud Computing Services” , Spanning, Dec. 17, 2021 https://spanning.com/blog/cloud-computing-benefits-disadvantages-types/
- DIGITIMES. “醫療、保健、照護加防疫 健康照護上雲端” https://www.digitimes.com.tw/iot/article.asp?cat=130&id=355732 (瀏覽日期：2022 年 8 月 22 日)
- INSIDE. “電子病歷上雲法規正式上路！Epic Cloud 帶醫療業齊聚上雲” https://www.inside.com.tw/article/28368-epic-cloud (瀏覽日期：2022 年 8 月 22 日)
- INFINITIES. “為何混合雲成為雲端技術的主流選擇？” https://blog.infinix.co/tw/2022/05/13/%E7%82%BA%E4%BD%95%E6%B7%B7%E5%90%88%E9%9B%B2%E6%88%90%E7%82%BA%E9%9B%B2%E7%AB%AF%E6%8A%80%E8%A1%93%E7%9A%84%E4%B8%BB%E6%B5%81%E9%81%B8%E6%93%87 (瀏覽日期：2022 年 8 月 22 日)
- EET 電子工程專輯 . “甲骨文助巨大集團 厚植數位行銷實力、提升購買體驗” https://www.eettaiwan.com/20180416np22/ (瀏覽日期：2022 年 8 月 22 日)
- PwC. “Operation Cloud Hopper” https://www.pwc.co.uk/cyber-security/pdf/pwc-uk-operation-cloud-hopper-report-april-2017.pdf (瀏覽日期：2022 年 8 月 24 日)
- Tara Seals. “Ex-Cisco Employee Convicted for Deleting 16K Webex Accounts” https://threatpost.com/cisco-employee-convicted-deleting-webex-accounts/162246/ (瀏覽日期：2022 年 9 月 6 日)
- Wikipedia. “Google services outages” https://en.wikipedia.org/wiki/Google_services_outages (瀏覽日期：2022 年 9 月 6 日)
- Lars Klint. “Azure Cosmos DB breach: What happened with ChaosDB?” https://acloudguru.com/blog/engineering/azure-cosmos-db-breach-what-happened-with-chaosdb (瀏覽日期：2022 年 9 月 6 日)
- Alex Scroxton. “AWS fixes vulnerabilities in Log4Shell hot patch” https://www.computerweekly.com/news/252516112/AWS-fixes-vulnerabilities-in-Log4Shell-hot-patch (瀏覽日期：2022 年 9 月 9 日)
- iThome. “【資安日報】2022 年 4 月 21 日，AWS 雲端服務的 Log4Shell 漏洞曾出現修補不全的狀況、勒索軟體 REvil 疑死灰復燃” https://www.ithome.com.tw/news/150544 (瀏覽日期：2022 年 9 月 9 日)
- Carlos Cervantes, Chris Villemez and Roberto Rosas. “AWS Outage Analysis: July 28, 2022” https://www.thousandeyes.com/blog/aws-outage-analysis-july-28-2022 (瀏覽日期：2022 年 9 月 9 日)
- 網管人 . “雲端後門洞開外洩資料　組態設定錯誤成最大元兇” https://www.netadmin.com.tw/netadmin/zh-tw/viewpoint/E616474B610B4CCAAB5E0BC3E7745D3C (瀏覽日期：2022 年 9 月 11 日)
- Fugue. “The State of Cloud Security 2021 Report” https://resources.fugue.co/state-of-cloud-security-2021-report (瀏覽日期：2022 年 9 月 11 日)
- Kevin Townsend. “Survey Shows Reasons for Cloud Misconfigurations are Many and Complex” https://www.securityweek.com/survey-shows-reasons-cloud-misconfigurations-are-many-and-complex (瀏覽日期：2022 年 9 月 11 日)
- Check Point Software Technologies Ltd. “Top 15 Cloud Security Issues, Threats and Concerns” https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-

issues-threats-and-concerns/
(瀏覽日期：2022 年 9 月 11 日)

- NIST. “General Access Control Guidance for Cloud Systems: NIST Publishes SP 800-210”
https://csrc.nist.gov/News/2020/nist-publishes-sp-800-210-ac-guidance-for-cloud
(瀏覽日期：2022 年 9 月 13 日)
- Skyhigh Security. “What is Cloud Security?”
https://www.skyhighsecurity.com/content/skyhigh/en-us/cybersecurity-defined/what-is-cloud-security.html/
(瀏覽日期：2022 年 9 月 14 日)
- 金融監督管理委員會 “110 年 12 月份信用卡 “現金卡及電子支付機構業務資訊”
https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202202100002&toolsflag=Y&dtable=News
(瀏覽日期 : 2022 年 3 月 23 日)
- Elsa Lee “電子錢包好夯！各大百貨零售、餐飲業者究竟在打什麼算盤”
https://medium.com/wishmobile/%E9%9B%BB%E5%AD%90%E9%8C%A2%E5%8C%85%E5%A5%BD%E5%A4%AF-%E5%90%84%E5%A4%A7%E7%99%BE%E8%B2%A8%E9%9B%B6%E5%94%AE-%E9%A4%90%E9%A3%B2%E6%A5%AD%E8%80%85%E7%A9%B6%E7%AB%9F%E5%9C%A8%E6%89%93%E4%BB%80%E9%BA%BC%E7%AE%97%E7%9B%A4-b7430f0bcdae
(瀏覽日期 : 2022 年 3 月 23 日)
- FISC “台灣 Pay QR Code 共通支付打造行動支付新世代”
https://www.fisc.com.tw/Upload/d42ce73b-1b82-4f05-899a-f8435b74b9c7/TC/9103.pdf
(瀏覽日期 : 2022 年 3 月 23 日)
- ENISA “Security of Mobile Payments and Digital Wallets”
https://www.enisa.europa.eu/publications/mobile-payments-security
(瀏覽日期 : 2022 年 3 月 23 日)
- Zimperium “Financially Motivated Mobile Scamware Exceeds 100M installations”
https://blog.zimperium.com/dark-herring-android-scamware-exceeds-100m:-installations/
(瀏覽日期 : 2022 年 3 月 23 日)
- 藍立晴 “【五倍券資安之亂】郵局網頁大出包！資安專家：政府、企業要加強 DevSecOps 觀念”
https://buzzorange.com/techorange/2021/09/23/stimulus-vouchers-taiwan-pay-threat/
(瀏覽日期 : 2022 年 3 月 23 日)
- Ionut Ilascu “Apple Pay with VISA lets hackers force payments on locked iPhones”
https://www.bleepingcomputer.com/news/security/apple-pay-with-visa-lets-hackers-force-payments-on-locked-iphones/
(瀏覽日期 : 2022 年 3 月 23 日)
- 日經 “日本 7-11 手機支付被盜刷的經過”
https://www.cybersecurity-insiders.com/500k-stolen-from-7pay-app-due-to-insufficient-mobile-payment-security/
(瀏覽日期 : 2022 年 3 月 23 日)
- 黃肇祥 “LINE Pay 驚傳 13 萬筆「交易資料」外洩！台灣、日本用戶都遭殃”
https://3c.ltn.com.tw/news/46947
(瀏覽日期 : 2022 年 3 月 23 日)
- 全國法規資料庫 “電子支付機構資訊系統標準及安全控管作業基準辦法”
https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=G0380243
(瀏覽日期 : 2022 年 3 月 23 日)
- 植根法律 “信用卡業務機構辦理行動信用卡業務安全控管作業基準”
https://www.rootlaw.com.tw/LawContent.aspx?LawID=A040390041061000-1070409
(瀏覽日期 : 2022 年 3 月 23 日)
- 行動資安應用聯盟 “行動應用 App 基本資安檢測基準”
https://www.mas.org.tw/storage/files/7284/original/1036571163c8afc445ce5.pdf
(瀏覽日期 : 2022 年 3 月 23 日)
- 財金公司 “支付卡產業資料安全標準 (PCI DSS) 之探討及實地查核分享 ”
https://www.fisc.com.tw/Upload/727606e2-2b6d-450a-a519-950191c11010/TC/12.pdf
(瀏覽日期 : 2022 年 3 月 23 日)

TWCERTCC台灣電腦網路危機暨處理協調中心
105台北市松山區八德路四段123號3樓
Taiwan Computer Emergency Response Team Coordination Center
3F.,No.123, Sec. 4, Bade Rd., Songshan Dist., Taipei City 105305, Taiwan (R.O.C)

1010100 1010111 1000011

1000101 1010010 1010100

www.twcert.org.tw/tw +886-2-2528-6768